THÈSE

PRÉSENTÉE À

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Alan HERTGEN**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

MODÈLES DE NÉRON ET GROUPES FORMELS

Soutenue le 18 mars 2016 à l'Institut de Mathématiques de Bordeaux
après avis de

Dino LORENZINI	Professeur, University of Georgia
Matthieu ROMAGNY	Professeur, Université de Rennes 1

devant le jury de thèse composé de

Michel EMSALEM	Professeur, Université de Lille 1 (Président)
Qing LIU	Professeur, Université de Bordeaux (Directeur)
Matthieu ROMAGNY	Professeur, Université de Rennes 1
Dajano TOSSICI	Maître de conférences, Université de Bordeaux

Remerciements

Je remercie Qing Liu d'avoir dirigé ma thèse avec disponibilité. Il m'a amené à réfléchir à des questions très intéressantes et a su réorienter mon travail aux moments nécessaires.

Je remercie Dino Lorenzini et Matthieu Romagny d'avoir rapporté ma thèse et pour leurs nombreuses remarques et corrections qui m'ont permis d'améliorer le manuscrit.

Je remercie Michel Emsalem, Matthieu Romagny et Dajano Tossici d'avoir accepté d'être membres de mon jury de thèse.

Je remercie Dino Lorenzini pour ses remarques à propos d'une version préliminaire de l'article qui constitue le chapitre 2 de cette thèse et les discussions que nous avons eues sur le sujet.

Je remercie Lars Halvard Halle de m'avoir invité une semaine à Copenhague et pour l'intérêt qu'il a porté à mon travail.

Je n'oublie pas les doctorants de l'I.M.B. avec qui j'ai passé d'excellents moments au cours de ces années de thèse.

Table des matières

Introduction

Modèles de Néron

Les modèles de Néron sont un outil central dans l'étude de la géométrie et de l'arithmétique des variétés abéliennes. Pour motiver leur définition, considérons l'exemple d'une courbe elliptique E sur le corps des nombres rationnels $\mathbb{Q}$ définie par une équation de Weierstrass

$$y^2 = x^3 - 2x^2 + 6.$$

Le discriminant de cette courbe elliptique est $\Delta = -2^6 \cdot 3 \cdot 5 \cdot 13$. Pour tout nombre premier $p \notin \{2, 3, 5, 13\}$, l'équation obtenue en réduisant les coefficients modulo p est celle d'une courbe elliptique sur le corps fini $\mathbb{F}_p$. Pour $p = 2$, on obtient l'équation

$$y^2 = x^3$$

qui est celle d'une courbe cuspidale sur $\mathbb{F}_2$. Pour $p = 3$, on obtient l'équation

$$y^2 = x^3 + x^2$$

qui est celle d'une courbe nodale sur $\mathbb{F}_3$. De même pour $p \in \{5, 13\}$, les courbes obtenues sont nodales. En considérant ensemble la courbe $E/\mathbb{Q}$ ainsi que les courbes obtenues par réduction sur $\mathbb{F}_p$, pour tout nombre premier p, on obtient un schéma projectif

$$\mathcal{W} = \operatorname{Proj} \mathbb{Z}[x, y, z]/(y^2z - x^3 + 2x^2z - 6z^3).$$

D'après le critère valuatif de propreté, on a la propriété suivante

$$\mathcal{W}(\mathbb{Z}) = E(\mathbb{Q}).$$

Cependant, $\mathcal{W}$ n'est pas lisse sur $\mathbb{Z}$ (aux nombres premiers $p \in \{2, 3, 5, 13\}$). On peut alors considérer le lieu lisse $\mathcal{E}^0$ de $\mathcal{W}$ sur $\mathbb{Z}$ mais dans ce cas

$$\mathcal{E}^0(\mathbb{Z}) \neq E(\mathbb{Q}).$$

On aimerait disposer d'un schéma $\mathcal{E}$ lisse sur $\mathbb{Z}$, mais non nécessairement projectif, tel que l'on ait la propriété

$$\mathcal{E}(\mathbb{Z}) = E(\mathbb{Q}).$$

C'est le rôle joué par le modèle de Néron de $E/\mathbb{Q}$. Il s'agira en fait d'un schéma en groupes lisse sur $\mathbb{Z}$ dont le schéma $\mathcal{E}^0/\mathbb{Z}$ défini ci-dessus sera la composante neutre.

On peut maintenant donner la définition d'un modèle de Néron. Considérons A une variété abélienne sur un corps global K (corps des fractions d'un anneau de Dedekind). Le *modèle de Néron* de A/K est un schéma en groupes $\mathcal{A}$ lisse sur l'anneau des entiers $\mathcal{O}_K$ qui vérifie la *propriété de Néron*, i.e.

$$\mathcal{A}(X) = A(X_K)$$

pour tout schéma X lisse sur $\mathcal{O}_K$, où $X_K = X \times_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} K$. On a notamment $\mathcal{A}(\mathcal{O}_K) = A(K)$ comme désiré. L'existence d'un tel modèle, qui est unique à unique isomorphisme près via la propriété ci-dessus, a été démontrée par André Néron en 1964 dans [Né64]. Raynaud a ensuite montré que la notion de modèle de Néron peut être étendue à certains groupes algébriques non nécessairement propres, notamment aux variétés semi-abéliennes (extensions d'une variété abélienne par un tore). Néron a lui-même utilisé ces modèles pour étudier la hauteur de points rationnels sur les variétés abéliennes. Depuis, les modèles de Néron ont été utilisés à de nombreuses fins, arithmétiques, comme dans la formulation de la conjecture de Birch et Swinnerton-Dyer, ou géométriques, comme dans l'étude des compactifications des espaces de modules de variétés abéliennes.

La démonstration de l'existence d'un modèle de Néron sur un corps global se fait en commençant par le cas local. Considérons une variété abélienne A sur un corps muni d'une valuation discrète K et $\mathcal{A}$ son modèle de Néron sur l'anneau des entiers $\mathcal{O}_K$. Soit k le corps résiduel de $\mathcal{O}_K$. On définit la réduction de A/K comme étant la fibre spéciale

$$\mathcal{A}_k = \mathcal{A} \times_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} k.$$

On dispose alors d'une application de réduction

$$A(K) = \mathcal{A}(\mathcal{O}_K) \to \mathcal{A}_k(k).$$

Le schéma $\mathcal{A}_k$ est lisse sur k mais non nécessairement propre ni même connexe. Considérons la composante neutre $\mathcal{A}_k^0$ de $\mathcal{A}_k$. Alors, on dispose d'une suite exacte

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi(A) \to 0$$

où $\Phi(A)$ est un schéma en groupes fini étale sur k appelé *groupe des composantes*. La composante neutre $\mathcal{A}_k^0/k$ est une extension d'une variété abélienne par un groupe algébrique linéaire connexe, c'est la décomposition de Chevalley. De plus, un groupe algébrique linéaire connexe commutatif est un produit direct d'un groupe unipotent par un tore. Dans le cas où la partie unipotente est triviale, on dit que A/K a *réduction semi-abélienne*. Supposons que K soit strictement hensélien. Alors, un résultat fondamental dû à Grothendieck assure qu'il existe une unique extension finie séparable minimale L/K telle que $A \times_K L/L$ ait réduction semi-abélienne.

Contenu de la thèse

Chapitre 1

On donne les définitions des objets utilisés dans cette thèse ainsi que les principaux résultats les concernant et dont on se sert par la suite. L'ordre est essentiellement celui d'apparition dans le texte.

Chapitre 2

Les résultats de ce chapitre sont contenus dans l'article [Her16] à paraître dans International Journal of Number Theory. On y répond à certaines questions posées par Liu et Lorenzini dans [LL01].

Soit K un corps muni d'une valuation discrète, complet et de corps résiduel k algébriquement clos. Soit A/K une variété abélienne et soit $\mathcal{A}/\mathcal{O}_K$ son modèle de Néron. On dit que A/K a *réduction scindée* si la suite exacte

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi(A) \to 0$$

est scindée. On dit que A/K a *réduction totalement non scindée* si aucun point d'ordre p de $\Phi(A)$, où p est la caractéristique de k, ne se relève en un point d'ordre p de $\mathcal{A}_k$.

Supposons que A/K soit de rang torique nul (i.e. la partie torique de $\mathcal{A}_k^0$ est triviale). Liu et Lorenzini ont montré que si A/K obtient réduction semi-abélienne sur une extension L/K modérément ramifiée (on dira que A/K est *modérément ramifiée*) alors A/K a réduction scindée. On montre que ce résultat ne se généralise pas sans l'hypothèse de rang torique nul en construisant un exemple de variété abélienne modérément ramifiée mais non scindée (§2.3.4). Pour cela, on considère une extension modérément ramifiée L/K et un élément $q \in L^\times$. À cet élément q est associé une courbe de Tate E/L dont on considère la restriction de Weil $A = \operatorname{Res}_{L/K} E$. Cette variété abélienne est le quotient rigide analytique du tore $T = \operatorname{Res}_{L/K} \mathbb{G}_{m,L}$ par le réseau $\Lambda = \operatorname{Res}_{L/K} q^{\mathbb{Z}}$. Alors que la réduction potentielle de A/K est déterminée par le tore T/K, on détermine une condition sur le réseau Λ/K (plus précisément sur q) tel que A/K n'ait pas réduction scindée.

On montre ensuite que si A/K est la variété jacobienne d'une courbe projective lisse C/K de genre g alors, pour toute extension M/K modérément ramifiée de degré plus grand qu'une constante ne dépendant que de g, la variété $A \times_K M/M$ a réduction scindée (corollaire 2.5.4). Cela étend les résultats de Liu et Lorenzini concernant les courbes elliptiques ainsi qu'un certain type de tores qui seront appelés *tores quotients* dans la suite. Pour cela, on utilise la filtration d'Edixhoven sur la fibre spéciale de $\mathcal{A}/\mathcal{O}_K$. Halle et Nicaise ont montré dans [HN16] que les sauts de cette filtration sont rationnels et que leur dénominateur commun est l'indice de stabilisation de C/K (voir §2.5.2 pour la définition). De plus, ils ont montré avec Eriksson dans [EHN15] que le nombre de sauts non nuls est égal à la dimension de la partie unipotente U de $\mathcal{A}_k^0/k$. Soit M/K une extension modérément ramifiée et soit $\mathcal{A}'/\mathcal{O}_M$ le modèle de Néron de $A \times_K M/M$. D'après la propriété de Néron on a un morphisme

$$\mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_M \to \mathcal{A}'$$

qui induit un morphisme

$$\mathcal{A}_k \to \mathcal{A}'_k.$$

Les résultats mentionnés ci-dessus nous permettent de montrer que si le degré de l'extension M/K est strictement supérieur à l'indice de stabilisation de C/K alors U/k est exactement le noyau de ce morphisme. On utilise alors un second résultat de [HN16] concernant l'effet d'un changement de base sur le groupe des composantes pour obtenir que $A \times_K M/M$ a réduction scindée. Pour finir, un théorème d'Artin et Winters permet de remplacer l'indice de stabilisation de C/K par une constante ne dépendant que de g.

Enfin, Liu et Lorenzini ont montré que le conducteur de Swan d'une courbe elliptique ou d'un tore quotient qui a réduction totalement non scindée est borné par une constante ne dépendant que de la dimension de la variété considérée. Toujours en considérant des restrictions de Weil de courbes elliptiques, on construit une famille de variétés abéliennes simples et de rangs toriques nuls qui ont réduction scindée et dont les conducteurs de Swan ne peuvent pas être bornés indépendamment du corps de définition (§2.6.3). Ils ont aussi montré que pour un corps K de caractéristique nulle, tout tore quotient sur K, dont le conducteur de Swan est plus grand qu'une constante ne dépendant que de la dimension et de l'indice de ramification absolu de K, a réduction scindée. On donne un exemple de variété abélienne de conducteur maximal (i.e. atteignant la borne de [BK94]) mais qui a réduction totalement non scindée (§2.6.5). Ces exemples montrent que ces deux derniers résultats ne se généralise pas sans plus d'hypothèse aux variétés abéliennes. Ces constructions reposent sur un lemme de [Mil72] qui permet d'exprimer le conducteur de Swan de la restriction de Weil $\mathrm{Res}_{L/K}\, E$ d'une courbe elliptique

E/L en fonction du conducteur de Swan $\delta(E/L)$ de E/L et de la différente $\mathcal{D}_{L/K}$ de l'extension L/K.

Chapitre 3

Soit K un corps muni d'une valuation discrète, complet et de caractéristique 0. Soit π_K une uniformisante de K. Soit A/K une variété abélienne de dimension g. Le noyau de l'application de réduction

$$A_1(K) = \mathrm{Ker}(A(K) \to \mathcal{A}_k(k))$$

est un groupe formel commutatif sur $\mathcal{O}_K$ dont on note la loi F. On s'intéresse dans ce chapitre à déterminer le plus grand voisinage π_K-adique de l'origine 0 dans $A_1(K)$ qui soit analytiquement isomorphe au polydisque $(\pi_K\mathcal{O}_K)^g$ muni de sa structure de groupe additif usuelle. On dispose de l'application logarithme

$$\log_F : A_1(K) \to (\pi_K\mathcal{O}_K)^g$$

qui est un isomorphisme local. L'obstruction à l'existence de l'isomorphisme souhaité est l'éventuelle non-trivialité du noyau de cette application. Or, celui-ci est le sous-groupe des points de torsion de $A_1(K)$. Il suffit donc de pouvoir mesurer les points de torsion du groupe formel. Dans le cas des courbes elliptiques, un résultat de Serre utilisant les polygones de Newton permet de contrôler ces points si la réduction est semi-abélienne (proposition 3.3.1). Si la réduction n'est pas semi-abélienne, une étude de l'effet d'un changement de base sur le groupe formel permet de se ramener au cas précédent et fait apparaître le conducteur de changement de base de Chai et Yu dans la formule que l'on obtient (proposition 3.3.4). Nous n'avons pas pu étendre cette méthode au cas de la dimension supérieure.

Chapitre 4

Soit K un corps muni d'une valuation discrète et de caractéristique 0. Dans le but d'approfondir le lien entre le modèle de Néron d'une variété abélienne A/K et son groupe formel, nous avons été amenés à étudier l'article [Fal08]. Dans celui-ci, Faltings définit une notion plus souple de modèle de Néron en ne demandant plus que tous les points étales de A/K s'étendent en des points de $\mathcal{A}/\mathcal{O}_K$ mais seulement un certain sous-ensemble. De ce point de vue, tout schéma en groupe lisse, de type fini et séparé sur $\mathcal{O}_K$ est un modèle de Néron de sa fibre générique. On s'est alors intéressé à l'étude des modèles des groupes additif $\mathbb{G}_{a,K}/K$ et multiplicatif $\mathbb{G}_{m,K}/K$ et plus précisément aux possibilités pour le groupe des composantes de tels modèles. Dans les démonstrations, on donne un procédé basé sur la notion de dilatation permettant d'obtenir toutes ces possibilités selon la caractéristique résiduelle et le type de réduction (propositions 4.2.1, 4.2.3, 4.3.1 et 4.3.2). Pour finir, on donne une borne pour le rang de la partie p-primaire du groupe des composantes géométriquement connexes de tels modèles dans le cas où K est une extension finie du corps des nombres p-adiques $\mathbb{Q}_p$ (propositions 4.4.3 et 4.4.4). Pour cela on montre que le groupe des composantes géométriquement connexes d'un modèle s'injecte dans celui du modèle obtenu à partir de $\mathbb{G}_{a,\mathcal{O}_K}$ ou $\mathbb{G}_{m,\mathcal{O}_K}$ en dilatant tous les points rationnels de la fibre spéciale un certain nombre de fois.

Chapitre 5

Ce dernier chapitre est assez disjoint des précédents et concerne la notion de conducteur efficace d'une courbe C/K introduite par Liu et Saito dans [LS00]. Les auteurs ont montré que, si la fibre spéciale du modèle propre régulier minimal de C/K n'est pas une fibre multiple, alors ce conducteur efficace est borné par le conducteur d'Artin. Dans le cas d'une courbe elliptique d'un type de réduction donné, ils obtiennent un encadrement du conducteur efficace en fonction du conducteur d'Artin. On montre ici que cet encadrement est optimal et que le conducteur efficace ne peut pas s'exprimer uniquement en fonction du conducteur d'Artin (proposition 5.3).

Chapitre 1

Prérequis

Le but de ce chapitre est d'introduire les objets nécessaires à la lecture de cette thèse et de fixer leur notation. Il ne contient pas de résultat original et très peu de démonstrations mais des références vers la littérature.

1.1 Restriction de Weil

Pour plus de détails on pourra consulter [BLR90, Section 7.6].

Définition 1.1.1. Soit $S' \to S$ un morphisme de schémas. Soit X' un schéma sur S'. On appelle *restriction de Weil de X' selon le morphisme $S' \to S$*, et on note $\operatorname{Res}_{S'/S} X'$, le schéma sur S représentant le foncteur sur les schémas sur S défini par

$$T \mapsto \operatorname{Hom}_{S'}(T \times_S S', X'),$$

si il existe.

Théorème 1.1.2. *Si X'/S' est quasi-projectif et si $S' \to S$ est fini et localement libre alors $\operatorname{Res}_{S'/S} X'$ existe.*

On se place dans les conditions du théorème pour la suite du paragraphe.

À partir de l'isomorphisme

$$\operatorname{Hom}_S(T, \operatorname{Res}_{S'/S} X') \cong \operatorname{Hom}_{S'}(T \times_S S', X')$$

on obtient deux morphismes importants. En considérant le morphisme identité sur $\operatorname{Res}_{S'/S} X'$ on obtient un morphisme

$$(\operatorname{Res}_{S'/S} X') \times_S S' \to X'. \tag{1.1}$$

De même, en considérant le morphisme identité sur $X' = X \times_S S'$, où X est un schéma sur S, on obtient un morphisme

$$X \to \mathrm{Res}_{S'/S}(X \times_S S'). \tag{1.2}$$

De plus, ce morphisme est une immersion fermée.

La notion de restriction de Weil est fonctorielle et commute au produit fibré. Ainsi la restriction de Weil d'un schéma en groupes est aussi un schéma en groupes.

Enfin, la notion de restriction de Weil commute avec le changement de base au sens suivant. Si $T \to S$ est un morphisme de changement de base et si on écrit $T' = T \times_S S'$ alors pour tout schéma X'/S' on a un isomorphisme canonique

$$\mathrm{Res}_{T'/T}(X' \times_{S'} T') \cong (\mathrm{Res}_{S'/S} X') \times_S T.$$

Soit K un corps et soit L/K une extension finie séparable de degré d. Soit X/L une variété quasi-projective de dimension g. La restriction de Weil $\mathrm{Res}_{L/K} X$ de X selon l'extension L/K est une variété quasi-projective de dimension $d \cdot g$. De plus, pour toute extension galoisienne M/K contenant L on a

$$(\mathrm{Res}_{L/K} X) \times_K M \cong \prod_{\sigma} {}^{\sigma}(X \times_L M)$$

où le produit est indexé par les K-plongements $\sigma : L \to M$.

Si $X = \mathrm{Spec}\, L\,[x_1, \ldots, x_n]\,/(f_1, \ldots, f_m)$ est affine, alors la variété $\mathrm{Res}_{L/K} X$ peut être décrite explicitement. Soit $e_1, \ldots, e_d$ une base de L sur K. On écrit, pour tout $i \in \{1, \ldots, n\}$,

$$x_i = \sum_{j=1}^{d} y_{ij} e_j.$$

En remplaçant les x_i dans chaque f_k, pour tout $k \in \{1, \ldots, m\}$, on obtient

$$f_k(x_1, \ldots, x_n) = F_{k,1} e_1 + \cdots + F_{k,d} e_d,$$

avec $F_{k,\ell}$ un polynôme de $K[y_{ij}]$. Alors, on a

$$\mathrm{Res}_{L/K} X = \mathrm{Spec}\, K[y_{ij}]/(F_{k,\ell}).$$

Exemple 1.1.3. Soient $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$ une extension quadratique de K. On considère $\mathbb{G}_{m,L} = \mathrm{Spec}\, L[x, y]/(xy - 1)$. En posant

$$x = x_1 + x_2\sqrt{d},$$
$$y = y_1 + y_2\sqrt{d},$$

on obtient

$$(x_1 y_1 + d x_2 y_2 - 1) + (x_1 y_2 + x_2 y_1)\sqrt{d} = 0.$$

Ainsi, $\mathrm{Res}_{L/K} \mathbb{G}_{m,L}$ a pour variété sous-jacente la surface dans $\mathbb{A}^4_K$ définie par les équations

$$x_1 y_1 + d x_2 y_2 - 1 = 0,$$
$$x_1 y_2 + x_2 y_1 = 0.$$

1.2 Groupes algébriques commutatifs

Soit K un corps. On note K^s une clôture séparable de K, $\Gamma_K = \mathrm{Gal}(K^s/K)$ le groupe de Galois absolu de K et $\bar{K}$ une clôture algébrique de K.

Définition 1.2.1. Un *groupe algébrique* G/K est un schéma en groupes lisse sur K.

Remarque 1.2.2. Un groupe algébrique G/K est automatiquement séparé comme schéma.

Proposition 1.2.3. *Soit G/K un groupe algébrique. Alors, on a une suite exacte*

$$0 \to G^0 \to G \to \pi_0(G) \to 0$$

où G^0 est la composante connexe de G contenant 0 et $\pi_0(G)$ est un schéma en groupes étale sur K.

Définition 1.2.4. On appelle $\pi_0(G)$ le *groupe des composantes* de G/K.

Remarque 1.2.5. Un groupe algébrique connexe G/K est automatiquement de type fini et géométriquement intègre.

On distingue deux types de groupes algébriques.

Définition 1.2.6. On appelle

(1) *groupe algébrique linéaire* un groupe algébrique affine,

(2) *variété abélienne* un groupe algébrique connexe propre.

La terminologie *linéaire* vient du fait que les groupes algébriques affines correspondent aux sous-groupes algébriques fermés de $\mathrm{GL}(n)/K$. La terminologie *abélienne* vient du fait que les groupes algébriques connexes propres sont automatiquement commutatifs.

Deux exemples fondamentaux de groupes algébriques linéaires sont les groupes unipotents et les tores.

Définition 1.2.7. Soit G/K un groupe algébrique. On dit que G/K est *unipotent* si $G_{\bar{K}}/\bar{K}$ admet une suite de composition dont les quotients successifs sont isomorphes à des sous-groupes algébriques de $\mathbb{G}_{a,\bar{K}}/\bar{K}$.

Les groupes unipotents correspondent aux sous-groupes algébriques fermés du groupe $\mathbb{U}(n)/K$ formé des matrices triangulaires supérieures avec 1 sur la diagonale.

Définition 1.2.8. Soit G/K un groupe algébrique. On dit que G/K est un *tore* si G_{K^s}/K^s est isomorphe à un produit de copies de $\mathbb{G}_{m,K^s}/K^s$. Un tore est dit *déployé* s'il est isomorphe à un produit de copies de $\mathbb{G}_{m,K}/K$.

On donne maintenant trois exemples de tores qui apparaîtront dans le chapitre suivant. Soit L/K une extension finie séparable de degré d.

Exemple 1.2.9. Soit T/L un tore de dimension g. Alors, la restriction de Weil $(\operatorname{Res}_{L/K} T)/K$ est un tore de dimension $d \cdot g$.

Exemple 1.2.10. On dispose d'une application de norme

$$\operatorname{Res}_{L/K} \mathbb{G}_{m,L} \stackrel{\operatorname{Norm}_{L/K}}{\longrightarrow} \mathbb{G}_{m,K}$$

dont la construction est analogue à celle utlisée dans la démonstration de [ELL96, Theorem 1] pour les variétés abéliennes. Le noyau de cette application est un tore qui sera appelé *tore de norme de l'extension* L/K et noté $\operatorname{Res}^1_{L/K} \mathbb{G}_{m,L}$. C'est un tore de dimension $d-1$. On a

$$(\operatorname{Res}^1_{L/K} \mathbb{G}_{m,L})(K) = \left\{ z \in L^\times \mid \operatorname{Norm}_{L/K}(z) = 1 \right\}.$$

Exemple 1.2.11. Le quotient de l'immersion fermée (1.2)

$$\mathbb{G}_{m,K} \to \operatorname{Res}_{L/K} \mathbb{G}_{m,L}$$

est un tore qui sera appelé *tore quotient*. C'est un tore de dimension $d-1$.

Pour étudier les tores, on introduit la notion de caractère.

Définition 1.2.12. Soit T/K un tore. On définit le *groupe des caractères* de T/K comme

$$X(T) = \operatorname{Hom}_{K^s}(T_{K^s}, \mathbb{G}_{m,K^s}).$$

Si T/K est de dimension n, alors $X(T)$ est un groupe abélien libre de rang n muni d'une action de Γ_K. L'importance du groupe des caractères réside dans le théorème suivant.

Théorème 1.2.13. *On a une équivalence de catégories*

$$\begin{array}{rcl} \{\textit{Tores}/K\} & \leftrightarrow & \{\textit{Groupes abéliens libres de rang fini avec action de } \Gamma_K\} \\ T & \mapsto & X(T) \end{array}$$

Exemple 1.2.14. Soit L/K une extension finie séparable et soit M/K sa clôture galoisienne. Soient $\Gamma = \operatorname{Gal}(M/K)$ et $\Delta = \operatorname{Gal}(M/L)$. Le groupe des caractères du tore $\operatorname{Res}_{L/K} \mathbb{G}_{m,L}$ est le module de permutation $\mathbb{Z}[\Gamma/\Delta]$.

Exemple 1.2.15. Avec les notations de l'exemple précédent, soit $\{\delta_1, \ldots, \delta_n\}$ une base de $\mathbb{Z}[\Gamma/\Delta]$. Le groupe des caractères du tore de norme $\mathrm{Res}^1_{L/K}\,\mathbb{G}_{m,L}$ est le conoyau du morphisme $\mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}[\Gamma/\Delta]$ définit par $\varepsilon(1) = \sum_{i=1}^{n} \delta_i$.

Exemple 1.2.16. Avec les notations des exemples précédents, le groupe des caractères du tore quotient $(\mathrm{Res}_{L/K}\,\mathbb{G}_{m,L})/\mathbb{G}_{m,K}$ est le noyau du morphisme $\mathbb{Z}[\Gamma/\Delta] \xrightarrow{r} \mathbb{Z}$ définit par $r\left(\sum_{i=1}^{n} m_i\delta_i\right) = \sum_{i=1}^{n} m_i$.

Remarque 1.2.17. On peut montrer que le groupe des caractères du tore quotient est isomorphe au dual du groupe des caractères du tore de norme de l'extension L/K (voir [LL01, Lemma 4.1]). On dit que le tore quotient $(\mathrm{Res}_{L/K}\,\mathbb{G}_{m,L})/\mathbb{G}_{m,K}$ est le *tore dual* du tore de norme $\mathrm{Res}^1_{L/K}\,\mathbb{G}_{m,L}$.

Ces exemples fondamentaux de groupes algébriques sont en fait les briques de base de la théorie. En effet, la structure des groupes algébriques commutatifs connexes sur un corps parfait est donnée par le théorème suivant dû à Claude Chevalley.

Théorème 1.2.18 (Chevalley)**.**
Soit K un corps parfait et soit G/K un groupe algébrique (lisse) commutatif connexe. Il existe une unique suite exacte

$$0 \to H \to G \to A \to 0$$

où H/K est un groupe linéaire et A/K une variété abélienne.

De plus, un groupe algébrique linéaire connexe commutatif H/K peut être décomposé comme le produit direct d'un groupe unipotent U/K par un tore T/K.

On termine ce paragraphe sur la définition d'un objet central de cette thèse.

Définition 1.2.19. On dira qu'un groupe algébrique G/K est une *variété semi-abélienne* si c'est une extension d'une variété abélienne par un tore.

1.3 Courbes algébriques

Soit K un corps. Soit C/K une courbe (variété algébrique de dimension 1) projective. On note $\mathrm{Pic}^0(C)$ le sous-groupe de $\mathrm{Pic}(C)$ formé des classes de faisceaux inversibles sur C de degré 0.

Théorème 1.3.1. *Soit C/K une courbe projective lisse géométriquement connexe de genre g. Alors, il existe une variété abélienne J/K de dimension g telle que pour toute extension L/K on a un morphisme injectif*

$$\mathrm{Pic}^0(C_L) \hookrightarrow J(L)$$

qui est un isomorphisme si $C(L) \neq \emptyset$.

Définition 1.3.2. On appelle J/K la *variété jacobienne* de C/K, aussi notée $\mathrm{Jac}(C)/K$.

On considère maintenant le cas particulier des courbes de genre 1.

Définition 1.3.3. Une *courbe elliptique* E/K est une courbe projective lisse géométriquement connexe de genre 1 munie d'un point rationnel $0 \in E(K)$.

Le théorème suivant fournit d'autres définitions parfois utilisées des courbes elliptiques.

Théorème 1.3.4. *On a une bijection entre les classes d'isomorphisme des objets suivants :*

(1) *courbes elliptiques sur K,*

(2) *variétés abéliennes de dimension 1 sur K,*

(3) *courbes projectives lisses sur K, isomorphes à une sous-variété fermée de $\mathbb{P}^2_K$ définie par une* équation de Weierstrass

$$y^2z + a_1xyz + a_3xz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{1.3}$$

avec le point rationnel privilégié $(0 : 1 : 0)$.

Démonstration. La démonstration repose sur le théorème de Riemann-Roch et le fait qu'une courbe elliptique est canoniquement isomorphe à sa variété jacobienne. □

On rappelle les définitions des quantités suivantes associées à une équation de Weierstrass (1.3) :

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j(E) &= c_4^3/\Delta
\end{aligned} \tag{1.4}$$

Le fait qu'une courbe définie par une équation de Weierstrass soit lisse s'exprime par la non nullité du *discriminant* Δ.

1.4 Réduction des variétés algébriques

Soit K un corps muni d'une valuation discrète. Soit $\mathcal{O}_K$ l'anneau des entiers de K. La théorie de la réduction s'intéresse à étendre une variété algébrique V/K en un schéma $\mathcal{V}/\mathcal{O}_K$ qui possède de bonnes propriétés. La réduction de V/K est alors la fibre de $\mathcal{V}/\mathcal{O}_K$ au dessus du point fermé de $\operatorname{Spec} \mathcal{O}_K$. On dispose de modèles très intéressants dans le cas où V/K est une courbe projective lisse ou une variété semi-abélienne.

1.4.1 Réduction des variétés semi-abéliennes

En général, on ne peut pas étendre une variété abélienne sur K en un schéma propre et lisse sur $\mathcal{O}_K$. En relâchant l'hypothèse de propreté on obtient la notion de modèle de Néron.

Définition 1.4.1. Soit G/K un groupe algébrique commutatif. Un *modèle de Néron* de G/K est un schéma lisse et séparé $\mathcal{G}/\mathcal{O}_K$ muni d'un isomorphisme $\mathcal{G} \times_{\mathcal{O}_K} K \to G$ tel que, pour tout schéma lisse $X/\mathcal{O}_K$, l'application canonique

$$\operatorname{Hom}_{\mathcal{O}_K}(X, \mathcal{G}) \to \operatorname{Hom}_K(X \times_{\mathcal{O}_K} K, G)$$

est une bijection.

Remarque 1.4.2. La propriété universelle ci-dessus est appelée *propriété de Néron.* Elle implique qu'un modèle de Néron, s'il existe, est unique à unique isomorphisme près. Elle implique aussi que la structure de groupe algébrique commutatif sur G/K s'étend en une structure de schéma en groupes commutatif sur $\mathcal{G}/\mathcal{O}_K$.

Le théorème suivant est du à André Néron dans le cas abélien et Michel Raynaud pour la généralisation (voir [BLR90, Theorem 10.2.2]).

Théorème 1.4.3. *Toute variété semi-abélienne G/K admet un modèle de Néron.*

Contrairement aux modèles de Néron des variétés abéliennes, les modèles de Néron des variétés semi-abéliennes ne sont en général pas de type fini mais seulement localement de type fini. Par exemple le modèle de Néron de $\mathbb{G}_{m,K}/K$ dont la construction est donné dans [BLR90, Example 10.1.5] n'est pas de type fini. Ainsi on rencontre parfois la notation *modèle de Néron lft* pour préciser qu'il s'agit d'une extension de la notion définie par André Néron. Dans la suite, on ne fera pas la distinction.

Soit k le corps résiduel de K que l'on suppose algébriquement clos. Soit G/K une variété semi-abélienne et soit $\mathcal{G}/\mathcal{O}_K$ son modèle de Néron. On définit la *fibre spéciale* de G/K par

$$\mathcal{G}_k = \mathcal{G} \times_{\mathcal{O}_K} k.$$

On a une suite exacte

$$0 \to \mathcal{G}_k^0 \to \mathcal{G}_k \to \Phi(G) \to 0$$

où $\mathcal{G}_k^0/k$ est la composante connexe de $\mathcal{G}_k/k$ qui contient 0 et $\Phi(G)$ est le groupe des composantes de $\mathcal{G}_k/k$. Dans la suite, on identifiera $\Phi(G)$ avec le groupe abélien de type fini $\Phi(G)(k)$. On note que le morphisme de spécialisation

$$G(K) \cong \mathcal{G}(\mathcal{O}_K) \to \mathcal{G}_k(k)$$

induit un isomorphisme

$$G(K)/\mathcal{G}^0(\mathcal{O}_K) \cong \Phi(G)$$

lorsque K est hensélien.

Comme $\mathcal{G}_k^0/k$ est un groupe algébrique commutatif connexe, il existe une unique suite exacte

$$0 \to U \times T \to \mathcal{G}_k^0 \to A \to 0$$

où U/k est un groupe algébrique unipotent, T/k est un tore et A/k est une variété abélienne. Ceci permet d'attacher certains entiers à la variété semi-abélienne G/K.

Définition 1.4.4. Soit G/K une variété semi-abélienne et soit $\mathcal{G}/\mathcal{O}_K$ son modèle de Néron. On définit les rangs unipotent u_K, torique t_K et abélien a_K de G/K comme étant les dimensions de U/k, T/k et A/k respectivement dans la suite exacte ci-dessus.

Le cas particulier où la partie unipotente est triviale joue un rôle important.

Définition 1.4.5. Soit G/K une variété semi-abélienne et soit $\mathcal{G}/\mathcal{O}_K$ son modèle de Néron. On dira que G/K a *réduction semi-abélienne* si $\mathcal{G}_k^0/k$ est une variété semi-abélienne, i.e. si $u_K = 0$.

On a alors le résultat suivant.

Proposition 1.4.6. *[HN10, Proposition 4.1]*
Soit G/K une variété semi-abélienne. Soient G_{tor}/K et G_{ab}/K les parties torique et abélienne de G/K respectivement. Alors, G/K a réduction semi-abélienne si et seulement si G_{ab}/K a réduction semi-abélienne et G_{tor}/K est déployé.

On fixe K^s une clôture séparable de K et on note $\Gamma_K = \mathrm{Gal}(K^s/K)$ le groupe de Galois absolu de K. Le théorème suivant est dû à Alexandre Grothendieck dans le cas abélien (voir [SGA7, Théorème IX.3.6] et [HN16, Theorem 2.3.6.5 (2)]).

Théorème 1.4.7 (Théorème de réduction semi-stable)**.**
On suppose que K est hensélien. Soit G/K une variété semi-abélienne. Il existe une unique extension finie minimale L de K dans K^s telle que $G \times_K L$ ait réduction semi-abélienne. De plus, l'extension L/K est une extension galoisienne.

De plus, on dispose d'un critère galoisien de réduction semi-stable. On rappelle que le module de Tate de G/K est défini par

$$T_\ell(G) = \varprojlim_n G(K^s)[\ell^n]$$

où $G(K^s)[\ell^n]$ désigne le sous-groupe de ℓ^n-torsion de $G(K^s)$.

Théorème 1.4.8. *[HN16, Theorem 2.3.6.5 (1)]*
La variété semi-abélienne G/K a réduction semi-stable si et seulement si l'action de Γ_K sur le module de Tate $T_\ell(G)$ est unipotente.

Remarque 1.4.9. La formation des modèles de Néron ne commute pas au changement de base. Soit $\mathcal{O}_L$ un anneau de valuation discrète dominant $\mathcal{O}_K$ et soit L son corps des fractions. On note $\mathcal{G}'/\mathcal{O}_L$ le modèle de Néron de $G_L = G \times_K L$. Comme $\mathcal{G} \times_{\mathcal{O}_K} \mathcal{O}_L$ est lisse, la propriété de Néron implique l'existence d'un unique morphisme

$$h : \mathcal{G} \times_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{G}'$$

qui étend l'isomorphisme canonique entre les fibres génériques. En général, il est difficile de décrire les propriétés de ce morphisme. Par contre, si G/K a réduction semi-abélienne alors h est une immersion ouverte et donc induit un isomorphisme entre les composantes neutres (voir [SGA7, Corollaire IX.3.3]). Enfin, on notera que le morphisme h induit dans tous les cas un morphisme entre les groupes des composantes

$$\Phi(G) \to \Phi(G_L).$$

1.4.2 Réduction des courbes algébriques

Définition 1.4.10. Soit C/K une courbe projective, lisse et connexe. Un *modèle* de C/K est un schéma propre et plat $\mathcal{C}/\mathcal{O}_K$ muni d'un isomorphisme $\mathcal{C} \times_{\mathcal{O}_K} K \to C$.

Étant donnée une courbe algébrique C/K, il existe de nombreux modèles $\mathcal{C}/\mathcal{O}_K$. Dans la suite, on s'intéressera en particulier aux modèles réguliers et à croisements normaux. On rappelle la définition de ces derniers.

Définition 1.4.11. On dit qu'un modèle $\mathcal{C}/\mathcal{O}_K$ de C/K est *à croisements normaux* si $\mathcal{C}/\mathcal{O}_K$ est régulier et si la fibre spéciale $\mathcal{C}_k/k$ est un diviseur à croisements normaux de $\mathcal{C}/O_K$.

À l'intérieur de ces classes de modèles, il en existe des canoniques qui sont les modèles minimaux. On renvoie à [Liu02, §9.3] pour un exposé détaillé de la théorie des modèles minimaux. On dispose du résultat suivant.

Théorème 1.4.12. *Soit C/K une courbe projective, lisse et connexe de genre $g \geq 1$. Alors, C/K admet unique modèle minimal régulier et un unique modèle minimal à croisements normaux.*

Soit E/K une courbe elliptique. Alors, E/K admet un modèle minimal régulier $\mathcal{C}/\mathcal{O}_K$ en tant que courbe algébrique ainsi qu'un modèle de Néron $\mathcal{E}/\mathcal{O}_K$ en tant que variété abélienne. Il existe un lien entre ces deux modèles donné par le théorème suivant.

Théorème 1.4.13. *Le modèle de Néron $\mathcal{E}/\mathcal{O}_K$ de E/K est isomorphe au sous-schéma ouvert des points lisses de $\mathcal{C}/\mathcal{O}_K$.*

Pour terminer ce paragraphe, on mentionnera le fait que les fibres spéciales des modèles minimaux réguliers des courbes elliptiques se répartissent en un nombre fini de types selon la *classification de Kodaira-Néron*. On trouvera dans [Sil94, page 365] un tableau dans lequel sont regroupés les différents types de réduction avec notamment leurs symboles et le groupe des composantes du modèle de Néron correspondant. Quant aux courbes de genre supérieur, on leur associe une donnée combinatoire de la façon suivante. Soit X/K une courbe projective lisse et connexe de genre $g \geq 2$. Soit $\mathcal{X}/\mathcal{O}_K$ un modèle régulier de X/K. Soit

$$\mathcal{X}_k = \sum_{i=1}^{n} d_i \Gamma_i$$

la décomposition de $\mathcal{X}_k$ comme diviseur. Soit $K_{\mathcal{X}/\mathcal{O}_K}$ un diviseur canonique sur $\mathcal{X}$. On pose

$$k_i = K_{\mathcal{X}/\mathcal{O}_K} \cdot \Gamma_i$$

pour $i \in \{1, \dots, n\}$. Enfin, on note $M = (\Gamma_i \cdot \Gamma_j)_{1 \leq i,j \leq n}$ la matrice d'intersection de $\mathcal{X}_k$. On appelle *type* la donnée

$$(d_1, \dots, d_n, k_1, \dots, k_n, M).$$

On a alors les résultats suivant dus à Michael Artin et Gayn Winters.

Théorème 1.4.14. *[AW71, Theorem 1.6]*

Pour un genre $g \geq 2$ fixé, il n'existe qu'un nombre fini de types sans diviseur exceptionnel à un nombre fini de chaines de (-2)-courbes près.

Corollaire 1.4.15. *[AW71, Corollary 1.7]*

Les multiplicités d_i sont bornées par une fonction de g.

1.5 Conducteurs d'Artin et de Swan

On associe à une variété semi-abélienne ou à une courbe algébrique des conducteurs d'Artin et de Swan que l'on définit dans un premier temps dans le contexte plus général des représentations galoisiennes ℓ-adiques.

1.5.1 Définitions générales

On suit la présentation de [Ser85, §2.1]. Soit K un corps muni d'une valuation discrète. Soit k le corps résiduel de K supposé algébriquement clos de caractéristique $p \geq 0$. On fixe K^s une clôture séparable de K. On notera $\Gamma_K = \mathrm{Gal}(K^s/K)$ le groupe de Galois absolu de K. Soit ℓ un nombre premier différent de p. Soit V un $\mathbb{Q}_\ell$-espace vectoriel de dimension finie et soit

$$\rho : \Gamma_K \to \mathrm{Aut}(V)$$

une représentation ℓ-adique de Γ_K dans V.

Définition 1.5.1. On pose

$$\varepsilon(V) = \dim(V) - \dim(V^{\Gamma_K}).$$

On suppose dans la suite qu'il existe une extension finie galoisienne L/K dans K^s telle que l'action de Γ_L sur V soit unipotente. Pour tout entier $n \geq 0$, on définit V_n comme l'ensemble des $x \in V$ tels que $(\rho(\sigma) - 1)^n(x) = 0$ pour tout $\sigma \in \Gamma_L$. Si l'on pose

$$\mathrm{Gr}(V) = \bigoplus_{n \geq 0} V_{n+1}/V_n,$$

alors Γ_K agit sur $\mathrm{Gr}(V)$ par l'intermédiaire du groupe fini

$$\Gamma = \Gamma_K/\Gamma_L = \mathrm{Gal}(L/K).$$

On en déduit que, si $\sigma \in \Gamma_K$, la trace de $\rho(\sigma)$ dans V ne dépend que de l'image de σ dans Γ. On obtient ainsi une fonction

$$\mathrm{Tr}_\rho : \Gamma \to \mathbb{Q}_\ell.$$

Soit π_L une uniformisante de L et soit v_L la valuation sur L normalisée par $v_L(\pi_L) = 1$. On définit une fonction $b_\Gamma : \Gamma \to \mathbb{Z}$, appelée *caractère de Swan*, par

$$\begin{aligned} b_\Gamma(\sigma) &= 1 - v_L(\sigma(\pi_L) - \pi_L), \quad \text{si } \sigma \neq 1, \\ b_\Gamma(1) &= -\sum_{\sigma \neq 1} b_\Gamma(\sigma). \end{aligned}$$

Définition 1.5.2. Le *conducteur de Swan* de V est défini comme le produit scalaire

$$\delta(V) = |\Gamma|^{-1} \sum_{\gamma \in \Gamma} \mathrm{Tr}_\rho(\gamma) b_\Gamma(\gamma).$$

Le conducteur de Swan est un entier ≥ 0. Il est égal à 0 si et seulement si l'action de Γ_K sur $\mathrm{Gr}(V)$ est modérée, i.e. si $p = 0$ ou (dans le cas $p > 0$) si le p-Sylow de Γ_K agit trivialement sur $\mathrm{Gr}(V)$. Cette dernière condition signifie que le p-Sylow de Γ_K opère de façon unipotente sur V.

Définition 1.5.3. On définit l'*exposant du conducteur d'Artin* de V par

$$f(V) = \varepsilon(V) + \delta(V).$$

Dans la suite, on parlera simplement de *conducteur d'Artin.*

1.5.2 Cas des variétés semi-abéliennes

Soit G/K une variété semi-abélienne. Soit $T_\ell(G)$ le module de Tate de G/K et soit $V_\ell(G) = T_\ell(G) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. L'action de Γ_K sur $T_\ell(G)$ fournit une représentation ℓ-adique

$$\rho : \Gamma_K \to \mathrm{Aut}(V_\ell(G)).$$

Soient G_{tor}/K et G_{ab}/K les parties torique et abélienne de G/K respectivement. Il existe une extension finie galoisienne L/K dans K^s telle que Γ_L agit trivialement sur $T_\ell(G_{\mathrm{tor}})$ et de façon unipotente sur $T_\ell(G_{ab})$ (d'après le théorème de monodromie [SGA7, Théorème I.1.2] et le fait que $V_\ell(G_{ab})$ est isomorphe au dual du premier groupe de cohomologie étale ℓ-adique de $G_{ab} \times_K K^s$). On a une suite exacte

$$0 \to T_\ell(G_{\mathrm{tor}}) \to T_\ell(G) \to T_\ell(G_{ab}) \to 0.$$

Ainsi, Γ_L agit de façon unipotente sur $V_\ell(G)$. On peut donc définir $\varepsilon(V_\ell(G))$, $\delta(V_\ell(G))$ et $f(V_\ell(G))$. De plus, on peut montrer que $\varepsilon(V_\ell(G))$, $\delta(V_\ell(G))$ et $f(V_\ell(G))$ sont indépendants du choix de ℓ.

Définition 1.5.4. Soit G/K une variété semi-abélienne. On pose

$$\begin{aligned} \varepsilon(G/K) &= \varepsilon(V_\ell(G)), \\ \delta(G/K) &= \delta(V_\ell(G)), \\ f(G/K) &= f(V_\ell(G)), \end{aligned}$$

pour un nombre premier ℓ différent de p. On dira que $f(G/K)$ est le *conducteur d'Artin* de G/K et que $\delta(G/K)$ est le *conducteur de Swan* de G/K.

D'après le critère de réduction semi-abélienne, le conducteur de Swan $\delta(G/K)$ est égal à 0 si et seulement si G/K obtient réduction semi-abélienne après une extension finie modérément ramifiée L/K. Dans ce cas, on dira que G/K est une variété semi-abélienne *modérément ramifiée.*

Remarque 1.5.5. Soit T/K un tore. Soit ℓ un nombre premier différent de p. L'évaluation des caractères de T/K induit un isomorphisme galoisien entre $T\left[\ell^n\right](K^s)$ et $\mathrm{Hom}(X(T)/\ell^n X(T), \mathbb{G}_m\left[\ell^n\right](K^s))$. Il s'ensuit que, sous nos hypothèses sur K, le module de Tate $T_\ell(T)$ est isomorphe, en tant que module galoisien, au dual de $X(T) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Ainsi, on a $\delta(T/K) = \delta(X(T) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$ et $f(T/K) = f(X(T) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$. Le groupe des caractères permet donc de calculer les conducteurs d'Artin et de Swan de T/K.

Dans le cas abélien on dispose des résultats suivants.

Proposition 1.5.6. *[SGA7, §IV.4]*
Soit A/K une variété abélienne. Soient u_K et t_K les rang unipotent et torique de A/K. On a

$$\varepsilon(A/K) = t_K + 2u_K.$$

Proposition 1.5.7. *[ST68, Corollary 2.2]*
Soit A/K une variété abélienne de dimension g. Si $p > 2g + 1$ alors

$$\delta(A/K) = 0.$$

Soit E/K une courbe elliptique. Soit π_K une uniformisante de K et soit v_K la valuation sur K normalisée par $v_K(\pi_K) = 1$. La formule de Ogg-Saito relie la valuation du discriminant minimal de E/K, le conducteur d'Artin de E/K et le nombre de composantes irréductibles dans la fibre spéciale du modèle propre minimal régulier de E/K. Elle a été démontrée par Ogg ([Ogg67, Theorem 2]) par une analyse cas par cas excepté pour un corps K de caractéristique mixte $(0, 2)$, puis en général par Saito ([Sai88, Corollary 2]) comme cas particulier d'un résultat sur les courbes de genre $g \geq 1$.

Théorème 1.5.8 (Formule de Ogg-Saito)**.**
Soit E/K une courbe elliptique. Soient Δ le discriminant minimal de E/K et m le nombre de composantes irréductibles (géométriques) dans la fibre spéciale du modèle minimal régulier de E/K. On a

$$v_K(\Delta) = f(E/K) + m - 1.$$

1.5.3 Cas des courbes algébriques

Soit C/K une courbe projective, lisse et géométriquement connexe. On note $H^1(C_{K^s}, \mathbb{Q}_\ell)$ le premier groupe de cohomologie étale ℓ-adique de C. L'action de Γ_K sur $H^1(C_{K^s}, \mathbb{Q}_\ell)$ fournit une représentation ℓ-adique

$$\rho : \Gamma_K \to \mathrm{Aut}(H^1(C_{K^s}, \mathbb{Q}_\ell)).$$

Il existe une extension finie galoisienne L/K dans K^s telle que Γ_L agisse de façon unipotente sur $H^1(C_{K^s}, \mathbb{Q}_\ell)$ (d'après le théorème de monodromie [SGA7, Théorème I.1.2]). On peut donc définir $\varepsilon(H^1(C_{K^s}, \mathbb{Q}_\ell))$, $\delta(H^1(C_{K^s}, \mathbb{Q}_\ell))$ et $f(H^1(C_{K^s}, \mathbb{Q}_\ell))$. De plus, on peut montrer que ces entiers sont indépendants du choix de $\ell \neq p$.

Définition 1.5.9. Soit C/K une courbe projective, lisse et géométriquement connexe. On pose

$$\begin{aligned} \varepsilon(C/K) &= \varepsilon(H^1(C_{K^s}, \mathbb{Q}_\ell)), \\ \delta(C/K) &= \delta(H^1(C_{K^s}, \mathbb{Q}_\ell)), \\ f(C/K) &= f(H^1(C_{K^s}, \mathbb{Q}_\ell)), \end{aligned}$$

pour un nombre premier ℓ différent de p. On dira que $f(C/K)$ est le *conducteur d'Artin* de C/K et que $\delta(C/K)$ est le *conducteur de Swan* de G/K.

Remarque 1.5.10. On considère C/K une courbe projective, lisse et géométriquement connexe. Soit $J = \mathrm{Jac}(C)/K$ la variété jacobienne de C/K. Il découle des isomorphismes

$$H^1(C_{K^s}, \mathbb{Q}_\ell) \cong H^1(J_{K^s}, \mathbb{Q}_\ell)$$

et

$$H^1(J_{K^s}, \mathbb{Q}_\ell) \cong V_\ell(J)^\vee$$

que $\delta(C/K) = \delta(J/K)$ et $f(C/K) = f(J/K)$. Les conducteurs d'Artin et de Swan d'une courbe algébrique peuvent donc être calculés via sa variété jacobienne.

1.6 Uniformisation non-archimédienne

Soit K un corps muni d'une valuation discrète v_K. On suppose que K est complet.

Définition 1.6.1. Soit G/K une variété semi-abélienne. On dit qu'un sous-groupe analytique rigide fermé $\Lambda \subseteq G$ est un *réseau* s'il existe une extension finie séparable L/K telle que Λ_L/L est isomorphe au groupe constant $\mathbb{Z}^d$, où d est la dimension de la partie torique de G/K. On dit qu'un réseau Λ/K est *déployé* si c'est un groupe constant sur K.

Soit A/K une variété abélienne. Alors, A/K admet une uniformisation non-archimédienne au sens suivant (voir [BX96, Theorem 1.2]). Il existe une variété semi-abélienne G/K et un réseau Λ/K dans G/K tels qu'il existe une suite exacte de groupes analytiques rigides

$$0 \to \Lambda \to G \to A \to 0$$

et que G/K soit une extension algébrique

$$0 \to T \to G \to B \to 0$$

d'une variété abélienne B/K qui a potentiellement bonne réduction par un tore T/K.

Remarque 1.6.2. Soit L/K une extension finie séparable. Alors, A/K obtient réduction semi-abélienne sur L si et seulement si la variété abélienne B/K obtient bonne réduction sur L et le tore T/K et le réseau Λ/K sont déployés par une extension non ramifiée de L.

Exemple 1.6.3. On renvoie à [Sil94, Section 5.3] pour les détails. Soit $q \in K^*$ tel que $v_K(q) > 0$. On considère la courbe elliptique

$$E_q : y^2 + xy = x^3 + a_4 x + a_6$$

dont les coefficients sont donnés par les formules

$$a_4 = -5 \sum_{n \geq 1} \frac{n^3 q^n}{1 - q^n}, \quad a_6 = -\frac{1}{12} \sum_{n \geq 1} \frac{(7n^5 + 5n^3) q^n}{1 - q^n}.$$

La courbe E_q est appelé *courbe de Tate*. L'uniformisation non-archimédienne de E_q est donnée par une suite exacte

$$0 \to q^{\mathbb{Z}} \to \mathbb{G}_{m,K} \to E_q \to 0.$$

1.7 Groupes formels

On utilisera un point de vue assez naïf sans vraiment parler de géométries formelle ou analytique rigide.

1.7.1 Définitions et premières propriétés

Soit R un anneau commutatif unitaire.

Définition 1.7.1. Un *groupe formel de dimension n* est un n-uplet de séries formelles

$$F(X,Y) = (F_1(X,Y), \dots, F_n(X,Y)),$$

où $F_i(X,Y) \in R[[X_1,\dots,X_n,Y_1,\dots,Y_n]]$, tel que, pour tout $i \in \{1,\dots,n\}$, on ait

$$\begin{aligned} F_i(X,Y) &= X_i + Y_i + (\text{termes de degré } \geq 2), \\ F_i(X,F(Y,Z)) &= F_i(F(X,Y),Z) \ \ (\text{associativité}). \end{aligned}$$

On dira que le groupe formel est *commutatif* si pour tout $i \in \{1,\dots,n\}$ on a

$$F_i(X,Y) = F_i(Y,X) \ \ (\text{commutativité}).$$

Théorème 1.7.2 (Théorème des fonctions implicites formel)**.**
Soit $F(X,Y) \in R[[X_1,\dots,X_m,Y_1,\dots,Y_n]]^n$ un n-uplet de séries formelles sans terme constant et tel que la matrice jacobienne partielle J définie par

$$F(X,Y) \equiv JY \bmod (X_1,\dots,X_m, \textit{termes de degré } \geq 2)$$

soit inversible. Alors, il existe un unique n-uplet de séries formelles $f(X) \in R[[X_1,\dots,X_m]]^n$ tel que

$$F(X,f(X)) = 0.$$

Ainsi, étant donné un groupe formel $F(X,Y)$, il existe un unique n-uplet de séries formelles $\iota(X)$ en n indéterminées et sans terme constant tel que

$$F(X,\iota(X)) = 0 = F(\iota(X),X).$$

Le n-uplet $\iota(X)$ s'interprète comme l'élément symétrique de X. Ainsi, un groupe formel est en quelque sorte une loi de groupe sans ensemble sous-jacent.

Exemple 1.7.3. Le *groupe formel additif de dimension n* est donné par

$$\hat{\mathbb{G}}_a^n(X,Y) = X + Y.$$

Exemple 1.7.4. Le *groupe formel multiplicatif de dimension* 1 est donné par

$$\hat{\mathbb{G}}_m(X,Y) = X + Y + XY = (1+X)(1+Y) - 1.$$

Définition 1.7.5. Soient $F(X,Y)$ un groupe formel de dimension n et $G(X,Y)$ un groupe formel de dimension m. Un *morphisme*

$$F(X,Y) \to G(X,Y)$$

est un m-uplet de séries formelles $f(X)$ en n indéterminées et sans terme constant tel que

$$f(F(X,Y)) = G(f(X),f(Y)).$$

Définition 1.7.6. Un morphisme $f(X) : F(X,Y) \to G(X,Y)$ est un *isomorphisme* s'il existe un morphisme $g(X) : G(X,Y) \to F(X,Y)$ tel que

$$\begin{aligned} f(g(X)) &= X, \\ g(f(X)) &= X. \end{aligned}$$

Théorème 1.7.7 (Théorème d'inversion locale formel)**.**
Soient $F(X,Y)$ un groupe formel de dimension n et $G(X,Y)$ un groupe formel de dimension m. Un morphisme

$$f(X) : F(X,Y) \to G(X,Y)$$

est un isomorphisme si et seulement si la matrice jacobienne J définie par

$$f(X) \equiv JX \bmod (\textit{termes de degré } \geq 2)$$

est inversible.

Définition 1.7.8. On dira qu'un isomorphisme est *strict* si la matrice jacobienne J est égale à I_n.

Exemple 1.7.9. On considère les groupes formels $\hat{\mathbb{G}}_a(X,Y)$ et $\hat{\mathbb{G}}_m(X,Y)$ sur $\mathbb{Q}$ et les séries formelles

$$\begin{aligned} \exp(X) &= \sum_{n\geq 1} \frac{X^n}{n!}, \\ \log(1+X) &= \sum_{n\geq 1} (-1)^{n+1}\frac{X^n}{n}. \end{aligned}$$

Alors, $\exp(X) : \hat{\mathbb{G}}_a(X,Y) \to \hat{\mathbb{G}}_m(X,Y)$ et $\log(1+X) : \hat{\mathbb{G}}_m(X,Y) \to \hat{\mathbb{G}}_a(X,Y)$ définissent des isomorphismes stricts inverses l'un de l'autre.

Définition 1.7.10. Soit $F(X,Y)$ un groupe formel commutatif. Pour tout $n \in \mathbb{Z}$ on définit un morphisme

$$[n]_F(X) : F(X,Y) \to F(X,Y),$$

appelé *multiplication par n*, par récurrence via $[0]_F(X) = 0$, $[n+1]_F(X) = F([n]_F(X), X)$ et $[n-1]_F(X) = F([n]_F(X), \iota(X))$.

Lemme 1.7.11. *Soit $F(X,Y)$ un groupe formel commutatif et soit $n \in \mathbb{Z}$, on a*

$$[n]_F(X) = nX + (\textit{termes de degré } \geq 2).$$

Corollaire 1.7.12. *Le morphisme $[n]_F(X) : F(X,Y) \to F(X,Y)$ est un isomorphisme si et seulement si $n \in R^\times$.*

Théorème 1.7.13 ($\mathbb{Q}$-théorème)**.**
Soit $F(X,Y)$ un groupe formel commutatif de dimension n sur une $\mathbb{Q}$-algèbre R. Alors, il existe un unique isomorphisme strict

$$\log_F(X) : F(X,Y) \to \hat{\mathbb{G}}_a^n(X,Y).$$

Démonstration. Voir [Haz78, Corollary 11.1.6]. □

Définition 1.7.14. On appelle la série formelle $\log_F(X)$ le *logarithme* du groupe formel $F(X,Y)$. La série formelle inverse est appelée l'*exponentielle* du groupe formel $F(X,Y)$ et notée $\exp_F(X)$.

Plus généralement, si $F(X,Y)$ est un groupe formel commutatif de dimension n sur un anneau R de caractéristique 0, alors $\log_F(X)$ désigne l'unique série formelle $f(X)$ à coefficients dans $R \otimes_{\mathbb{Z}} \mathbb{Q}$ telle que $f(X) = X +$ (termes de degré ≥ 2) et

$$F(X,Y) = f^{-1}(f(X) + f(Y)).$$

Exemple 1.7.15. Les séries formelles $\log(1+X)$ et $\exp(X)$ de l'exemple ci-dessus sont les séries logarithme et exponentielle du groupe formel multiplicatif $\hat{\mathbb{G}}_m(X,Y)$ sur $\mathbb{Q}$.

1.7.2 Groupe associé à un groupe formel

Soit R un anneau local complet. Soit $\mathfrak{m}$ son idéal maximal et soit $k = R/\mathfrak{m}$ son corps résiduel. Soit $F(X,Y)$ un groupe formel de dimension n sur R.

Définition 1.7.16. Le *groupe associé* à $F(X,Y)$, noté $F(\mathfrak{m})$, est constitué de l'ensemble $\mathfrak{m}^n$ muni de la loi

$$(x_1,\ldots,x_n) +_F (y_1,\ldots,y_n) = F(x_1,\ldots,x_n,y_1,\ldots,y_n).$$

Cette loi est bien définie puisque les séries convergent sur $\mathfrak{m}^n$ et elle munit l'ensemble $\mathfrak{m}^n$ d'une structure de groupe. Si de plus le groupe formel est commutatif alors $F(\mathfrak{m})$ est un groupe abélien.

Exemple 1.7.17. Le groupe additif $\hat{\mathbb{G}}_a^n(\mathfrak{m})$ est simplement le groupe $\mathfrak{m}^n$ muni de l'addition induite par l'addition sur R.

Exemple 1.7.18. Le groupe multiplicatif $\hat{\mathbb{G}}_m(\mathfrak{m})$ est isomorphe au groupe $1+\mathfrak{m}$ muni de la multiplication induite par la multiplication sur R.

On suppose dans la suite que les groupes formels sont commutatifs et on s'intéresse aux éléments de torsion dans les groupes abéliens associés.

Proposition 1.7.19. *Soit $p \geq 0$ la caractéristique de k. Alors, un élément de torsion de $F(\mathfrak{m})$ est d'ordre une puissance de p si $p > 0$ et trivial si $p = 0$.*

Démonstration. Il suffit de montrer que $F(\mathfrak{m})$ ne contient pas d'élément de torsion d'ordre premier à p. Soit $m \geq 1$ un entier premier à p. Soit $x \in F(\mathfrak{m})$ un élément tel que $[m]_F(x) = 0$. Comme m est premier à p, $m \in R^\times$ et donc

$$[m]_F(X) : F(X, Y) \to F(X, Y)$$

est un isomorphisme. Cela induit un isomorphisme

$$[m]_F : F(\mathfrak{m}) \to F(\mathfrak{m}).$$

En particulier, le noyau de cet isomorphisme est trivial et donc $x = 0$. D'où le résultat. □

On analyse maintenant plus précisément la torsion p-primaire dans le cas d'anneaux de valuation discrète. Pour cela, on aura besoin du lemme suivant.

Lemme 1.7.20. *Soit $F(X, Y)$ un groupe formel sur une $\mathbb{Z}_{(p)}$-algèbre R, où p est un nombre premier. Alors, il existe des séries formelles $g_0(X)$ et $g_1(X)$ telles que $g_0(X) = X + (\text{termes de degré } \geq 2)$, $g_1(0) = 0$ et*

$$[p]_F(X) = pg_0(X) + g_1(X^p).$$

Démonstration. Voir [Haz78, Remark 5.4.8] pour le cas de la dimension 1 qui se généralise aux dimensions supérieures. □

Soit $\mathcal{O}_K$ un anneau de valuation discrète complet de caractéristique 0. Soit π_K une uniformisante de $\mathcal{O}_K$ et soit $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$ son corps résiduel. Soit p la caractéristique de k que l'on suppose > 0. Soit v_K la valuation normalisée sur $\mathcal{O}_K$ telle que $v_K(\pi_K) = 1$. Le théorème suivant généralise [Sil86, Theorem IV.6.1]. La preuve est issue d'une version préliminaire de [CX08].

Théorème 1.7.21. *Soit $F(X, Y)$ un groupe formel sur $\mathcal{O}_K$ de dimension n. On suppose que $x = (x_1, \ldots, x_n) \in F(\pi_K\mathcal{O}_K)$ est d'ordre exactement p^m pour un certain entier $m \geq 1$. Alors, il existe un indice $i \in \{1, \ldots, n\}$ tel que*

$$v_K(x_i) \leq \frac{v_K(p)}{p^m - p^{m-1}}.$$

Démonstration. On remarque tout d'abord que pour toute série formelle $f(X) \in \mathcal{O}_K[[X]]$ sans terme constant et tout élément $x \in \mathfrak{m}^n$ on a

$$v_K(f(x)) \geq \inf_i \{v_K(x_i)\}.$$

On va démontrer le théorème par récurrence sur m.

Soit $x \neq 0$ tel que $[p]_F(x) = 0$. On peut supposer que $v_K(x_1) \leq v_K(x_i)$ pour tout $i \in \{1, \ldots, n\}$. Avec les notations du lemme précédent on a

$$0 = pg_0(x) + g_1(x^p).$$

En considérant la première composante de cette égalité, on a

$$0 = p(x_1 + h_0(x_1, \ldots, x_n)) + h_1(x_1^p, \ldots, x_n^p).$$

Or, on a $v_K(x_1) < v_K(h_0(x_1, \ldots, x_n))$ d'où

$$v_K(h_1(x_1^p, \ldots, x_n^p)) = v_K(p(x_1 + h_0(x_1, \ldots, x_n))) = v_K(px_1) = v_K(p) + v_K(x_1).$$

D'autre part, on a

$$v_K(h_1(x_1^p, \ldots, x_n^p)) \geq \inf_i \{v_K(x_i^p)\} = v_K(x_1^p) = pv_K(x_1).$$

On obtient ainsi

$$v_K(p) \geq (p-1)v_K(x_1),$$

ce qui démontre le résultat dans le cas $m = 1$.

On suppose que le résultat est vrai pour un entier $m \geq 1$. Soit $x \in F(\mathfrak{m})$ un élément d'ordre exactement p^{m+1}. Alors, l'élément $y = [p]_F(x)$ est d'ordre exactement p^m. On peut supposer que $v_K(y_1) \leq v_K(y_i)$ pour tout $i \in \{1, \ldots, n\}$. Par hypothèse de récurrence, on a

$$v_K(y_1) \leq \frac{v_K(p)}{p^m - p^{m-1}}.$$

Comme précédemment, on a

$$\begin{aligned} v_K(y_1) &\geq \inf \{v_K(h_1(x_1^p, \ldots, x_n^p)), v_K(p(x_1 + h_0(x_1, \ldots, x_n)))\} \\ &\geq \inf_i \{\inf \{v_K(px_i), v_K(x_i^p)\}\}. \end{aligned}$$

Comme $v_K(x_i) \geq 1$ et $m \geq 1$, il est impossible d'avoir $\dfrac{v_K(p)}{p^m - p^{m-1}} \geq v_K(px_i)$. Ainsi, pour un certain indice $i \in \{1, \ldots, n\}$ on doit avoir

$$\frac{v_K(p)}{p^m - p^{m-1}} \geq v_K(x_i^p),$$

ce qui achève la démonstration. □

Exemple 1.7.22. Soit $F(X, Y)$ un groupe formel sur $\mathbb{Z}_p$. Si $p \geq 3$, alors $F(p\mathbb{Z}_p)$ n'a pas d'élément de torsion non trivial. Si $p = 2$, les éléments de torsion sont d'ordre ≤ 2 et par exemple -1 est d'ordre 2 dans $\hat{\mathbb{G}}_m(2\mathbb{Z}_2) \cong 1 + 2\mathbb{Z}_2$.

1.8 Dilatations

Pour plus de détails on pourra consulter [BLR90, Section 3.2]. Soit $\mathcal{O}_K$ un anneau de valuation discrète. Soit π_K une uniformisante de $\mathcal{O}_K$ et $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$ son corps résiduel. Soit $X/\mathcal{O}_K$ un schéma de type fini et plat. Soit E un sous-schéma fermé de la fibre spéciale X_k défini par un faisceau d'idéaux $\mathcal{I} \subseteq \mathcal{O}_X$.

Définition 1.8.1. Soit $\widetilde{X} \to X$ l'éclatement de E dans X. On note $\mathcal{I}' = \mathcal{I} \cdot \mathcal{O}_{\widetilde{X}}$ et on définit

$$X' = \left\{ x \in \widetilde{X} \mid \mathcal{I}'_x \text{ est engendré par } \pi_K \right\}$$

qui est un sous-schéma ouvert de $\widetilde{X}$. On dit que $X' \to X$ est la *dilatation de E dans X.*

La dilatation $X' \to X$ satisfait la propriété universelle suivante : pour tout schéma $Z/\mathcal{O}_K$ plat, un morphisme $Z \to X$ se factorise par $X' \to X$ si et seulement si $Z_k \to X_k$ se factorise par $E \to X_k$.

Si $X = \operatorname{Spec} A$ est affine et $\mathcal{I} = (\pi_K, g_1, \ldots, g_n)$ alors X' est affine de fonctions globales

$$A\left[\frac{g_1}{\pi_K}, \ldots, \frac{g_n}{\pi_K}\right].$$

Si $X/\mathcal{O}_K$ est un schéma en groupes et si E/k est un sous-schéma en groupes de X_k/k alors $X'/\mathcal{O}_K$ est un schéma en groupes et le morphisme $X' \to X$ est un morphisme de schémas en groupes (voir [BLR90, Proposition 3.2.2 (d)]).

Si $X/\mathcal{O}_K$ est lisse et que le centre de la dilatation E/k est lisse, alors un calcul local montre que la dilatation X' de E dans X est lisse sur $\mathcal{O}_K$ (voir [BLR90, Proposition 3.2.3]). De plus, X' est égal au complémentaire dans $\widetilde{X}$ du transformé strict de la fibre spéciale X_k.

Soit K le corps de fractions de $\mathcal{O}_K$. La notion de dilatation va nous permettre de décomposer les morphismes entre modèles de groupes algébriques sur K. Plus précisément on a le résultat suivant.

Proposition 1.8.2. *[LLR04, Corollary 2.3]*

Soit $f : F \to G$ un morphisme de schémas en groupes sur $\mathcal{O}_K$ lisses et de type fini. On suppose que $f_K : F_K \to G_K$ est un isomorphisme. Si f est séparé, alors c'est la composée d'un nombre fini de dilatations de centres lisses sur k.

1.9 Faisceau des différentielles et faisceau canonique

On renvoie à [Liu02, Section 6.4.2] pour plus de détails.

Définition 1.9.1. Soient Y un schéma localement noethérien et $f : X \to Y$ un morphisme quasi-projectif localement d'intersection complète. Soit $i : X \to Z$ une immersion régulière dans Z qui est lisse sur Y. Soit $\mathcal{I}$ le faisceau d'idéaux qui définit i. On note $\mathcal{C}_{X/Z} = i^\star\mathcal{I}/\mathcal{I}^2$ le faisceau conormal de X dans Z et $\Omega^1_{Z/Y}$ le faisceau des différentielles relatives de X sur Y. On définit le *faisceau canonique* de $X \to Y$ comme étant le faisceau inversible

$$\omega_{X/Y} = \det(\mathcal{C}_{X/Z})^\vee \otimes_{\mathcal{O}_X} i^\star(\det \Omega^1_{Z/Y}).$$

Proposition 1.9.2. *Soient Y un schéma localement noethérien et $f : X \to Y$ un morphisme quasi-projectif localement d'intersection complète de dimension relative virtuelle $d \geq 0$. On a un morphisme canonique*

$$c_{X/Y} : \Omega^d_{X/Y} \to \omega_{X/Y}$$

qui coïncide avec l'identité sur le lieu lisse de f.

On peut décrire localement ce morphisme. Soit A un anneau noethérien. Soit $B = A[T_1, \ldots, T_n]/I$ où I est un idéal engendré par une suite régulière $F_1, \ldots, F_r$ avec $r \leq n$. Le faisceau $\omega_{\operatorname{Spec} B/\operatorname{Spec} A}$ est engendré par

$$(\bar{F}_1 \wedge \cdots \wedge \bar{F}_r)^\vee \otimes ((\mathrm{d}T_1 \wedge \cdots \wedge \mathrm{d}T_n) \otimes 1_B),$$

où $\bar{F}_i$ est l'image de F_i dans I/I^2. On note t_i l'image de T_i dans B. On a un morphisme canonique

$$c : \Omega^{n-r}_{B/A} \to H^0(\operatorname{Spec} B, \omega_{\operatorname{Spec} B/\operatorname{Spec} A})$$

tel que pour toute partie $S = \{j_{r+1}, \ldots, j_n\}$ de $\{1, \ldots, n\}$ on a

$$c(\mathrm{d}t_{j_{r+1}} \wedge \cdots \wedge \mathrm{d}t_{j_n}) = \Delta_S \cdot (\bar{F}_1 \wedge \cdots \wedge \bar{F}_r)^\vee \otimes ((\mathrm{d}T_1 \wedge \cdots \wedge \mathrm{d}T_n) \otimes 1_B)$$

où Δ_S est le déterminant de la matrice jacobienne $(\partial F_i/\partial T_j)_{i,j}$ dans laquelle on a retiré les colonnes $j_{r+1}, \ldots, j_n$.

Chapter 2

Splitting properties of the reduction of semi-abelian varieties

This chapter is a slightly different version of the paper [Her16] to appear in International Journal of Number Theory.

2.1 Introduction

Let K be a complete discrete valuation field. Let π_K be a uniformizing element of K. Let v_K be the discrete valuation on K normalized such that $v_K(\pi_K) = 1$. Let $\mathcal{O}_K$ be the ring of integers. Let k be the residue field which we assume to be algebraically closed of characteristic exponent $p \geq 1$. Let G/K be a semi-abelian variety with Néron (lft) model $\mathcal{G}/\mathcal{O}_K$ (see Définition 1.4.1 and Théorème 1.4.3). Let $\mathcal{G}_k = \mathcal{G} \times_{\mathcal{O}_K} k$ be the special fiber of $\mathcal{G}/\mathcal{O}_K$. We have an exact sequence

$$0 \to \mathcal{G}_k^0 \to \mathcal{G}_k \to \Phi(G) \to 0 \tag{2.1}$$

where $\mathcal{G}_k^0/k$ is the identity component of $\mathcal{G}_k/k$ and $\Phi(G)$ is the group of components which is known to be a finitely generated abelian group. Following [LL01, Introduction] we shall say that G/K has *split reduction* if this exact sequence is split. In other words, G/K has split reduction when $\mathcal{G}_k/k$ is isomorphic to the direct product $\mathcal{G}_k^0 \times_k \Phi(G)$ as an algebraic group. When $\Phi(G)$ is finite, G/K has split reduction if and only if for each $\varphi \in \Phi(G)$ there exists $x \in \mathcal{G}_k(k)$ lifting φ and with the same order.

We know that a semi-abelian variety G/K has split reduction when $p = 1$ (see [LL01, Proposition 1.4]), or when $\mathcal{G}_k^0/k$ is semi-abelian (see [LL01, Proposition 1.6]), or when G/K is a tamely ramified abelian variety (*i.e.* the minimal finite separable extension such that G/K acquires semi-abelian reduction is tamely ramified) with toric rank equal to 0 (see [LL01, Corollary 1.9]). This makes natural the question whether split reduction is automatic for tamely ramified semi-abelian varieties (this is [LL01, Question 1.10]).

Let us also recall the notion of totally not split semi-abelian variety from [LL01, §1.2]. We say that an exact sequence of abelian groups

$$0 \to H^0 \to H \to \Psi \to 0$$

is *totally not split* (for a fixed p) if for each $\varphi \in \Psi$ of order p there is no $x \in H$ of order p lifting φ. We say that a semi-abelian variety G/K has *totally not split reduction* if the exact sequence (2.1) is totally not split.

In [LL01], Liu and Lorenzini studied in detail the case of elliptic curves and norm tori together with their duals. For such a semi-abelian variety G/K, they found that there exists a constant c_1 depending only on the dimension of G/K such that if G/K has totally not split reduction then the Swan conductor (see Définition 1.5.4) of G/K is positive and bounded by c_1. For some classes of tori they found that there exists a constant c_2 depending only on the dimension of G/K and on the absolute ramification index $v_K(p)$ such that if the Swan conductor of G/K is greater than c_2 then G/K has split reduction. Finally, they found that there exists a constant c_3 depending only on the dimension of G/K such that G_M/M has split reduction for any tamely ramified extension M/K of degree greater than c_3. They ask whether similar statements hold in greater generality in [LL01, Questions 6.9, 6.10 and 6.11] respectively.

The aim of this chapter is to provide answers to these questions. We answer negatively [LL01, Question 1.10] in §2.3.4 by constructing a family of tamely ramified abelian varieties which do not have split reduction. We answer negatively [LL01, Questions 6.9] in §2.6.3 by constructing a family of simple abelian varieties which have totally not split reduction but whose Swan conductors cannot be bounded independently of the field of definition. We answer negatively [LL01, Questions 6.10] in §2.6.5 by constructing an abelian variety whose Swan conductor is as large as possible but which does not have split reduction. Finally, we give a positive answer to [LL01, Questions 6.11] with Corollary 2.5.4 which states that Jacobian varieties acquire split reduction after sufficiently large tamely ramified extensions. Our counterexamples are Weil restrictions of elliptic curves, so we give general considerations about splitting properties of Weil restrictions in Section 2.4.

2.2 A review of Liu and Lorenzini's results

2.2.1 The general case

Let us recall a few elementary results about the splitting properties. For an abelian group H, we will denote by H_{tors} the torsion subgroup of H, by H_p its

p-primary part and by $H[n]$ the subgroup of elements of order dividing n. When we use this notation for an algebraic group H/k we actually consider its group of closed points $H(k)$. First, let us give a proof of the following elementary lemma.

Lemma 2.2.1. *[LL01, Lemma 1.1]*
Let

$$0 \to H^0 \to H \xrightarrow{c} \Psi \to 0$$

be an exact sequence of commutative groups. Let $n \geq 1$ be an integer. Let J be a subgroup of H^0 such that $H^0 = J + nH^0$. Denote by $n_H : H \to H$ the multiplication-by-n map on H. Then,

$$c(n_H^{-1}(J)) = \Psi\,[n]\,.$$

Proof. The inclusion $c(n_H^{-1}(J)) \subseteq \Psi\,[n]$ is obvious since $J \subseteq \mathrm{Ker}(c)$. Let $\varphi \in \Psi[n]$. Let $x \in H$ be such that $c(x) = \varphi$. We have $n \cdot x \in H^0 = J + nH^0$. Let $j \in J$ and $y \in H^0$ be such that $n \cdot x = j + n \cdot y$. Then, $c(x - y) = \varphi$ and $n \cdot (x - y) = j \in J$ whence $\varphi \in c(n_H^{-1}(J))$. So we have the other inclusion. □

Proposition 2.2.2. *[LL01, Proposition 1.4]*
Let G/K be a semi-abelian variety. Let $\mathcal{G}/\mathcal{O}_K$ be its Néron model. Then we have the following properties :

(1) Let $\varphi \in \Phi(G)$ be an element of finite order n prime to p. Then, φ lifts to an element of $\mathcal{G}_k$ of order n.

(2) The sequence

$$0 \to \mathcal{G}^0_{k,p} \to \mathcal{G}_{k,p} \to \Phi(G)_p \to 0 \tag{2.2}$$

is exact.

(3) G/K has split reduction if and only if (2.2) is split.

(4) G/K has totally not split reduction if and only if (2.2) is totally not split.

Proof. (1) Since $p \nmid n$, the multiplication-by-n map on the smooth commutative group scheme $\mathcal{G}^0_k$ is surjective. We can apply Lemma 2.2.1 with $J = 0$ to the exact sequence (2.1).

(2) The only thing to prove is that $\mathcal{G}_{k,p} \to \Phi(G)_p$ is surjective. The algebraic group $\mathcal{G}^0_k/k$ is an extension of a semi-abelian variety by a unipotent group U/k. Since the multiplication-by-n map is surjective for any integer n on any semi-abelian variety, we have $\mathcal{G}^0_k = U + n\mathcal{G}^0_k$. Lemma 2.2.1 implies that any element $\varphi \in \Phi(G)[p^r]$ lifts to an element $x \in \mathcal{G}_k$ such that $p^r \cdot x \in U$. But U/k is killed by a power of p whence $x \in \mathcal{G}_{k,p}$.

(3) The condition is clearly necessary. Let us show that it is sufficient. The group of components $\Phi(G)$ is a finitely generated abelian group. So it is the direct sum of finitely many monogenous groups. Thus, to show that G/K has split reduction, it is enough to show that any element $\varphi \in \Phi(G)$ lifts to an element of $\mathcal{G}_k$ of the same order. If the order of φ is infinite then the assertion is clear. If the order of φ is a power of p then it follows from the hypothesis. Finally, if the order of φ is an integer n prime to p then it follows from (1).

(4) It follows from the definition.

□

A consequence of this proposition is that the matter of splitting is only non-trivial for $p > 1$, which we will assume from now on.

Corollary 2.2.3. *[LL01, Corollary 1.5]*
If $p \nmid |\Phi(G)_{\mathrm{tors}}|$, then G/K has split reduction.

Proof. It follows from Proposition 2.2.2 (3). □

Proposition 2.2.4. *[LL01, Proposition 1.6]*
Assume that G/K has semi-abelian reduction. Then, G/K has split reduction.

Proof. According to Proposition 2.2.2 (3), we need only to show that (2.2) is split. As in the proof of Proposition 2.2.2 (2), an element $\varphi \in \Phi(G)[p^r]$ lifts to an element $x \in \mathcal{G}_k$ such that $p^r \cdot x \in U$. By hypothesis $U = 0$, thus (2.2) is split. □

2.2.2 Tamely ramified semi-abelian varieties

Let G/K be a semi-abelian variety. There exists a minimal finite separable extension L/K such that $G_L = G \times_K L$ has semi-abelian reduction (see Théorème 1.4.7). Let G_{tor}/K and G_{ab}/K be the toric and the abelian parts of G/K. Note that $G_{\mathrm{tor}} \times_K L$ is a split torus (that is to say isomorphic to some power of $\mathbb{G}_{m,L}/L$) by Proposition 1.4.6. The following proposition is a combination of [LL01, Corollaries 1.7 and 1.9].

Proposition 2.2.5. *Let G/K be a semi-abelian variety whose abelian part G_{ab}/K has toric rank* 0. *Let L/K be the minimal finite separable extension such that G_L/L has semi-abelian reduction. If L/K is tamely ramified then G/K has split reduction.*

Proof. We adapt the proof of [HN16, Theorem 7.1.2.8]. By [HN16, Proposition 4.1.1.3], the sequence

$$\Phi(G_{\mathrm{tor}}) \to \Phi(G) \to \Phi(G_{\mathrm{ab}}) \to 0 \tag{2.3}$$

is exact. Now, $\Phi(G_{\mathrm{ab}})$ is killed by $[L:K]^2$ by [LL01, Proposition 1.8]. By [HN10, Corollary 5.4], the kernel of the canonical morphism $\Phi(G_{\mathrm{tor}}) \to \Phi(G_{\mathrm{tor}} \times_K L)$ is killed by $[L:K]$. As the group of components of a split torus is free, $\Phi(G_{\mathrm{tor}})_{\mathrm{tors}}$ is in the kernel of this morphism and hence is killed by $[L:K]$. Now, the exact sequence (2.3) implies that $\Phi(G)_{\mathrm{tors}}$ is killed by $[L:K]^3$ and in particular its order is prime to p. We have recalled in §2.2.1 that this implies that G/K has split reduction. □

Corollary 2.2.6. *Let E/K be an elliptic curve. Let L/K be the minimal finite separable extension such that E_L/L has semi-abelian reduction. If L/K is tamely ramified then E/K has split reduction.*

Proof. If E/K has semi-abelian (multiplicative or good) reduction then it follows from Proposition 2.2.4. Otherwise, the toric rank of E/K is 0 and it follows from Proposition 2.2.5. □

2.2.3 Two particular cases

Let us insist on two particular cases of Proposition 2.2.5. First, an abelian variety A/K which has potentially good reduction over a tamely ramified extension L/K has split reduction. Note that one can prove this using again [HN10, Corollary 5.4] and the fact that the group of components of an abelian variety with good reduction is trivial. Second, a torus T/K which splits over a tamely ramified extension L/K has split reduction. Indeed, T_L/L is isomorphic to a split torus if and only if T_L/L has semi-abelian reduction.

2.2.4 Non-Archimedean uniformization

Let us recall that an abelian variety A/K admits a non-Archimedean uniformization as follows (see Section 1.6). There exist a semi-abelian variety G/K and a lattice Λ/K in G/K such that the sequence of rigid analytic groups

$$0 \to \Lambda \to G \to A \to 0$$

is exact and such that G/K is an algebraic extension

$$0 \to T \to G \to B \to 0$$

of an abelian variety B/K with potentially good reduction by a torus T/K.

Let us denote by $\delta(G/K)$ the Swan conductor of G/K. Recall that $\delta(G/K)$ is zero if and only if G/K acquires semi-abelian reduction after a tamely ramified extension L/K. Considering this non-Archimedean uniformization and §2.2.3 it is natural to ask the following question.

Question 2.2.7. *[LL01, Question 1.10]*

Let G/K be a semi-abelian variety. Let L/K be the minimal finite separable extension such that G_L/L has semi-abelian reduction. If L/K is tamely ramified, is it true that G/K has split reduction ? In other words, is it true that the Swan conductor $\delta(G/K)$ is positive if G/K does not have split reduction ?

In spite of all this evidence, we will show that the answer to this question is no by constructing a family of counterexamples in §2.3.4. Note that we need to consider abelian varieties over K of dimension > 1 (by Corollary 2.2.6), positive toric rank (by Proposition 2.2.5) and which do not have semi-abelian reduction over K (by §2.2.1).

2.2.5 The case of elliptic curves

The main results in [LL01] about elliptic curves are gathered in the following theorem.

Theorem 2.2.8. *[LL01, Theorem 2.1 and Proposition 3.3]*

Let E/K be an elliptic curve and let $\delta(E/K)$ be its Swan conductor.

(1) If E/K has totally not split reduction, then

$$1 \leq \delta(E/K) \leq 3.$$

(2) If E/K has not split but not totally not split reduction, then E is of type $\mathbf{I}_{2n}^*$ for some integer n and

$$1 \leq \delta(E/K) \leq 2n + 3.$$

(3) Let M/K be a tamely ramified extension of degree ≥ 4. Then E_M/M has split reduction.

2.2.6 The case of quotient tori

Let L/K be a finite separable extension. Consider $\mathrm{Res}_{L/K}\,\mathbb{G}_{m,L}$, the Weil restriction of $\mathbb{G}_{m,L}/L$ under the extension L/K (see Section 1.1 for the definition and first properties of Weil restriction). Let S/K be the *quotient torus* $(\mathrm{Res}_{L/K}\,\mathbb{G}_{m,L})/\mathbb{G}_{m,K}$. Define the *norm torus* T/K, also denoted by $\mathrm{Res}^1_{L/K}\,\mathbb{G}_{m,L}$ in the sequel, to be the kernel of the norm map

$$\mathrm{Res}_{L/K}\,\mathbb{G}_{m,L} \overset{\mathrm{Norm}_{L/K}}{\longrightarrow} \mathbb{G}_{m,K}.$$

By [LL01, Lemma 4.1], S/K is isomorphic to the dual torus of T/K. Moreover, if L/K is a cyclic extension then S/K is isomorphic to T/K. The main results about tori in [LL01] are about this kind of tori and are gathered in the following theorem.

Theorem 2.2.9. *[LL01, Theorem 4.6 and Corollary 4.11]*
Let S/K be the quotient torus $(\mathrm{Res}_{L/K}\,\mathbb{G}_{m,L})/\mathbb{G}_{m,K}$ and let $\delta(S/K)$ be its Swan conductor.

(1) The torus S/K has totally not split reduction if and only if

$$1 \leq \delta(S/K) \leq \dim(S).$$

(2) If $\delta(S/K) \geq (\dim(S)+1)\mathrm{ord}_p(\dim(S)+1)v_K(p)$, then S/K has split reduction.

(3) Let M/K be a tamely ramified extension of degree $\geq \dim(S)+1$. Then, S_M/M has split reduction.

2.2.7 Some further questions

The results recalled in the last two theorems lead naturally to the following questions on possible generalizations.

Question 2.2.10. *[LL01, Question 6.9]*
Let g be a positive integer and consider all abelian varieties A of dimension g over a discrete valuation field K with toric rank equal to 0. Is there a constant c_1 depending on g but not on the field K such that if A/K has totally not split reduction then the Swan conductor $\delta(A/K)$ is bounded by c_1 ?

This question has a positive answer for elliptic curves (see Theorem 2.2.8 (1)) or for abelian varieties uniformized by quotient tori as above (see [LL01, Theorem 6.6] which relies on Theorem 2.2.9 (1)). As mentioned in [LL01, Question 6.9] one can construct obvious counterexamples by taking the product of an abelian variety with totally not split reduction by an elliptic curve with trivial group of components and large Swan conductor. We will construct in §2.6.3 a family of simple abelian varieties which have totally not split reduction and whose Swan conductors really depend on the field of definition so that the answer is no even for simple abelian varieties.

Question 2.2.11. *[LL01, Question 6.10]*
Assume that K is of characteristic 0. Let A/K be an abelian variety of dimension g. The Swan conductor of A/K is bounded by a constant depending on g and the absolute ramification index $v_K(p)$ only by [BK94, Proposition 6.2 and Proposition 6.11]. Is there a bound c_2 depending on g and $v_K(p)$ only such that if $\delta(A/K) > c_2$ then A/K has split reduction ?

Of course, we want c_2 to be smaller than the absolute bound of [BK94]. Such a bound exists for quotient tori (see Theorem 2.2.9 (2)) but we will show that the answer is no in general by giving in §2.6.5 an example of abelian variety whose

Swan conductor achieves the bound from [BK94] but which does not have split reduction. Let us however mention the following result which implies the existence of such a bound for elliptic curves.

Proposition 2.2.12. *Assume that K is of characteristic 0. Let E/K be an elliptic curve. If $\delta(E/K)$ achieves the bound from [BK94], then E/K has split reduction.*

Proof. If $p \neq 2, 3$, then E/K is tamely ramified and hence has split reduction by Corollary 2.2.6. If $p = 3$, then the bound of [BK94] is $3v_K(3) \geq 3$ (see also [LRS93]). Only elliptic curves with reduction type **III** or **III*** may not have split reduction and in this case we have $\delta(E/K) = 1$ or 2 by [LL01, §2.13 and §2.14], whence the result.

Let $p = 2$. In this case, the bound of [BK94] is $6v_K(2) > 3$ (see also [LRS93]). Therefore by Theorem 2.2.8 (1) an elliptic curve whose conductor achieves the bound of [BK94] does not have totally not split reduction. Assume that E/K does not have split reduction and that $\delta(E/K) = 6v_K(2)$. By Theorem 2.2.8 (b) we know that E/K has reduction type $\mathbf{I}_{2n}^*$ for some integer n. Now, we will follow the proof of [LL01, Proposition 2.11 (b)]. Let Δ be the minimal discriminant of E/K. Then [LL01, Proposition 2.11 (b)] implies that $v_K(\Delta) \leq 4n + 9$. Assume E/K is given by a minimal Weierstrass equation

$$y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathcal{O}_L$ for $i \in \{1, 2, 3, 4, 6\}$. As in [LL01], let us set $e = v_K(2)$ and $v = v_K(a_1)$. By Ogg's formula we have

$$\begin{aligned} v_K(\Delta) &= 2 + \delta(E/K) + (2n + 5 - 1) \\ &= 6e + 2n + 6. \end{aligned}$$

Consider first the case where $e < v$. We have $v_K(\Delta) > 4e + 2n + 6$. According to the table of valuations in [LL01], $4e + 2n + 6$ has to be greater or equal to $4n + 8$ or $3e + 3n + 7$. If $4e + 2n + 6 \geq 4n + 8$ then $2e \geq n + 1$ and $v_K(\Delta) \geq 5n + 9$ which is false. If $4e + 2n + 6 \geq 3e + 3n + 7$ then $e \geq n + 1$ and $v_K(\Delta) \geq 8n + 12$ which is false.

Consider the case where $e \geq v$. If $v = 1$, then $v_K(\Delta) = 2n + 8$ but this is false so that we can assume $v > 1$. We have $v_K(\Delta) > 4v + 2n + 4$. According to the table of valuations in [LL01], $4v + 2n + 4$ has to be greater or equal to $4n + 8$ or $3v + 3n + 6$. If $4v + 2n + 4 \geq 4n + 8$ then $2v \geq n + 2$ and $v_K(\Delta) \geq 5n + 12$ which is false. If $4v + 2n + 4 \geq 3v + 3n + 6$ then $v \geq n + 2$ and $v_K(\Delta) \geq 8n + 18$ which is false. Hence, there is a contradiction, i.e. $\delta(E/K) = 6v_K(2)$ implies that E/K has split reduction. $\square$

Question 2.2.13. *[LL01, Question 6.11]*

Let G/K be a semi-abelian variety of dimension g that does not have split reduction.

(1) Is it always possible to find a tamely ramified extension M/K such that G_M/M has split reduction ?

(2) Does there exist a constant c_3 depending on g only such that if M/K is any tamely ramified extension of degree greater than c_3, then G_M/M has split reduction ?

These questions have positive answers for elliptic curves or quotient tori (Theorem 2.2.8 (3) and Theorem 2.2.9 (3)). We will show that the answer to these questions is positive for Jacobian varieties over K in Corollary 2.5.4.

2.3 Splitting properties of tamely ramified semi-abelian varieties

2.3.1 Weil restriction

We recall below standard facts about Weil restrictions and we refer the reader to [BLR90, Section 7.6] for details. Let $S' \to S$ be a morphism of schemes. Let X' be a scheme over S'. The *Weil restriction* $\operatorname{Res}_{S'/S} X'$ *of* X' *under the morphism* $S' \to S$, when it exists, is the scheme over S representing the functor on schemes over S defined by

$$T \mapsto \operatorname{Hom}_{S'}(T \times_S S', X').$$

When X'/S' is quasi-projective and $S' \to S$ is finite and locally free then $\operatorname{Res}_{S'/S} X'$ always exists. The notion of Weil restriction commutes with base change in the following sense. If $T \to S$ is a morphism of base change and if we write $T' = T \times_S S'$ then for any scheme X'/S' there is a canonical isomorphism

$$\operatorname{Res}_{T'/T}(X' \times_{S'} T') \xrightarrow{\simeq} (\operatorname{Res}_{S'/S} X') \times_S T. \tag{2.4}$$

2.3.2 Weil restriction and Néron models

Let L/K be a finite separable extension of degree d. Let G/L be a semi-abelian variety of dimension g. Then $\operatorname{Res}_{L/K} G$ is a semi-abelian variety over K of dimension $d \cdot g$. Let $\mathcal{O}_L$ be the ring of integers of L. Let $\mathcal{G}/\mathcal{O}_L$ be the Néron model of G/L and let $\mathcal{G}^0/\mathcal{O}_L$ be its identity component. Then, $\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K} \mathcal{G}$ is the Néron model of $\operatorname{Res}_{L/K} G$ over $\mathcal{O}_K$ ([BLR90, Proposition 7.6.6]). The following proposition is inspired by [NX91, Lemma 3.1].

Proposition 2.3.1. *The identity component of* $\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}$ *is* $\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}^0$ *and we have the following isomorphism*

$$\Phi(\operatorname{Res}_{L/K} G) \xrightarrow{\simeq} \Phi(G).$$

Proof. It follows from [CGP10, Proposition A.5.9] that the fibers of $\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}^0$ are connected. From the immersion

$$\mathcal{G}^0 \to \mathcal{G}$$

we get a morphism

$$\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}^0 \to \operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}$$

which factorizes through

$$\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}^0 \to (\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G})^0.$$

Now, since the Weil restriction commutes with open and closed immersions by [BLR90, Proposition 7.6.2], we have

$$\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}^0 \xrightarrow{\simeq} (\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G})^0.$$

Finally, we have

$$\begin{array}{rcl}\Phi(\operatorname{Res}_{L/K} G) & \xleftarrow{\simeq} & (\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G})(\mathcal{O}_K)/(\operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{G}^0)(\mathcal{O}_K)\\ & \xrightarrow{\simeq} & \mathcal{G}(\mathcal{O}_L)/\mathcal{G}^0(\mathcal{O}_L)\\ & \xrightarrow{\simeq} & \Phi(G).\end{array}$$

□

2.3.3 Weil restriction of Tate curves

Let L/K be a finite separable extension of degree $d \geq 2$. Let π_L be a uniformizing element of L. Let v_L be the discrete valuation on L normalized such that $v_L(\pi_L) = 1$. Let $q \in L^\times$ be such that $v_L(q) > 0$ and let E/L be the Tate curve associated to q (see Exemple 1.6.3). Set $n = v_L(q)$. Let $\mathcal{E}/\mathcal{O}_L$ be the Néron model of E/L and let $\mathcal{E}^0/\mathcal{O}_L$ be its identity component. Let us recall that we have the following isomorphisms (see [Sil94, Section V.4])

$$\begin{array}{rcl}E(L) & \cong & L^\times/q^{\mathbb{Z}},\\ \mathcal{E}^0(\mathcal{O}_L) & \cong & \mathcal{O}_L^\times,\\ \Phi(E) & \cong & \mathbb{Z}/n\mathbb{Z}.\end{array}$$

Let us consider the abelian variety $A = \operatorname{Res}_{L/K} E/K$ obtained by Weil restriction under the extension L/K. In particular, $\dim(A) = d$. The Néron model of A over $\mathcal{O}_K$ is $\mathcal{A} = \operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K} \mathcal{E}$ (see §2.3.2) and its identity component is $\mathcal{A}^0 = \operatorname{Res}_{\mathcal{O}_L/\mathcal{O}_K} \mathcal{E}^0$ (by Proposition 2.3.1). The special fiber $\mathcal{E}^0_k/k$ is isomorphic to $\mathbb{G}_{m,k}/k$ (see [Sil94, Theorem V.5.3]), thus we have by the base change formula (2.4)

$$\mathcal{A}^0_k \cong \operatorname{Res}_{(\mathcal{O}_L/\pi_K\mathcal{O}_L)/k} \mathbb{G}_{m,(\mathcal{O}_L/\pi_K\mathcal{O}_L)}$$

and then

$$\mathcal{A}^0_k(k) \cong (\mathcal{O}_L/\pi_K\mathcal{O}_L)^\times.$$

As L/K is totally ramified, $\mathcal{O}_L$ is generated by π_L over $\mathcal{O}_K$ and π_L satisfies an Eisenstein equation

$$t^d + a_1 t^{d-1} + \cdots + a_d = 0$$

with $a_i \in \pi_K\mathcal{O}_K$ and $v_K(a_d) = 1$. As in the proof of [NX91, Proposition 3.2], we have a split exact sequence

$$0 \to 1 + \pi_L\mathcal{O}_L/\pi_K\mathcal{O}_L \to (\mathcal{O}_L/\pi_K\mathcal{O}_L)^\times \to k^\times \to 0. \tag{2.5}$$

The group $k^\times$ is the group of closed points of a one-dimensional torus over k and the group $1 + \pi_L\mathcal{O}_L/\pi_K\mathcal{O}_L$ is the group of closed points of a unipotent algebraic group over k. Indeed, one has the composition series

$$\{1\} = 1 + \pi_L^d\mathcal{O}_L/\pi_K\mathcal{O}_L \subseteq 1 + \pi_L^{d-1}\mathcal{O}_L/\pi_K\mathcal{O}_L \subseteq \cdots \subseteq 1 + \pi_L\mathcal{O}_L/\pi_K\mathcal{O}_L$$

whose succesive quotients are isomorphic to k. We may note that the toric rank of A/K is positive and that A/K does not have semi-abelian reduction so that we are in the required situation to deal with Question 2.2.7.

We can describe the reduction map $A(K) \to \mathcal{A}_k(k)$ (which is surjective because K is assumed to be complete). Let $P \in A(K) \cong E(L) \cong L^\times/q^{\mathbb{Z}}$. The image of P in $\Phi(A) \cong \Phi(E) \cong \mathbb{Z}/n\mathbb{Z}$ is given by the class of $v_L(z)$ modulo n where $z \in L^\times$ is a preimage of P. If $P \in \mathcal{A}^0(\mathcal{O}_K) \cong \mathcal{E}^0(\mathcal{O}_L) \cong \mathcal{O}_L^\times$ then its image in $\mathcal{A}^0_k(k) \cong (\mathcal{O}_L/\pi_K\mathcal{O}_L)^\times$ is given by reduction modulo $\pi_K\mathcal{O}_L$. In particular, the kernel of the reduction map is isomorphic to $1 + \pi_K\mathcal{O}_L$.

The next lemma is the analogue in our situation of [LL01, Claim 4.7] which is about quotient tori.

Lemma 2.3.2. *Let $m \in \mathbb{N}$ be a divisor of n. There exists a point in $\mathcal{A}_k(k)$ of order m whose image in $\Phi(A)$ is also of order m if and only if π_L^n/q is an m-th power in $(\mathcal{O}_L/\pi_K\mathcal{O}_L)^\times$.*

Proof. The existence of such a point is equivalent to the existence of $z \in L^\times$ such that

$$v_L(z) \equiv n/m \bmod n$$

and

$$z^m \in q^{\mathbb{Z}}(1+\pi_K\mathcal{O}_L).$$

Suppose that such z exists. Multiplying z by a suitable power of q we may suppose that $v_L(z) = n/m$. Thus, necessarily $z^m/q \in 1+\pi_K\mathcal{O}_L$ (recall that $v_L(q) = n$). Then

$$\pi_L^n/q = (\pi_L^{n/m}/z)^m(z^m/q) \in \mathcal{O}_L^m(1+\pi_K\mathcal{O}_L).$$

Conversely, if $\pi_L^n/q \equiv y^m \mod \pi_K\mathcal{O}_L$ for some $y \in \mathcal{O}_L^\times$, then we can take $z = y^{-1}\pi_L^{n/m}$. □

Corollary 2.3.3. *Assume that $v_L(q) = p$. Then, $A = \mathrm{Res}_{L/K} E/K$ has split reduction if and only if*

$$q/\pi_L^p \in \mathcal{O}_K^\times((1+\pi_L\mathcal{O}_L)^p + \pi_K\mathcal{O}_L). \tag{2.6}$$

Proof. This follows from the lemma and the exact sequence (2.5), using that the multiplication by p is surjective on $k^\times \cong (\mathcal{O}_K/\pi_K\mathcal{O}_K)^\times$. □

Remark 2.3.4. In some sense, both the conditions of having split reduction and not having split reduction for A/K as in Corollary 2.3.3 are open for the topology on L. Indeed, if we consider q' close enough to q, i.e. such that $q' \in q(1+\pi_K\mathcal{O}_L)$, then q satisfies condition (2.6) if and only if q' satisfies condition (2.6).

Proposition 2.3.5. *Let L/K be a Galois extension. Then A_L/L has purely multiplicative reduction.*

Proof. Recall that E/L has multiplicative reduction. Hence, the action of the absolute Galois group $\Gamma_L = \mathrm{Gal}(K^s/L)$ on the Tate module $T_\ell(E)$, $\ell \neq p$, is unipotent and non-trivial. Now, we have an isomorphism

$$A_L \cong \prod_{\sigma\in\mathrm{Gal}(L/K)} {}^\sigma E.$$

Let $\sigma \in \mathrm{Gal}(L/K)$. The action of Γ_L on $T_\ell({}^\sigma E)$ is conjugated to its action on $T_\ell(E)$ and thus is unipotent and non-trivial. This implies that ${}^\sigma E/L$ has multiplicative reduction which proves the proposition. □

2.3.4 Counterexample to Question 2.2.7

For any tamely ramified (hence Galois since k is algebraically closed) extension L/K, one can choose $q \in L^\times$ with $v_L(q) = p$ such that condition (2.6) is not satisfied (for instance take $q = \pi_L^p(1+\pi_L)$). This way, we get tamely ramified abelian varieties (by Proposition 2.3.5) which do not have split reduction (by Corollary 2.3.3) and this gives a negative answer to Question 2.2.7.

Remark 2.3.6. Using Lemma 2.3.2, one can construct abelian varieties with a specified subgroup of $\Phi(A)$ lifting into $\mathcal{A}_k(k)$. More precisely, let us fix two non-negative integers $m \leq n$. Then, let us take $q \in L^\times$ such that $v_L(q) = p^n$ so that we have $\Phi(A) \cong \mathbb{Z}/p^n\mathbb{Z}$. Now, if one choose $q \in L^\times$ such that

$$q/\pi_L^{p^n} \in \mathcal{O}_K^\times((1+\pi_L\mathcal{O}_L)^{p^m} + \pi_K\mathcal{O}_L)$$

but

$$q/\pi_L^{p^n} \notin \mathcal{O}_K^\times((1+\pi_L\mathcal{O}_L)^{p^{m+1}} + \pi_K\mathcal{O}_L)$$

then Lemma 2.3.2 implies that every element of order p^m lifts into $\mathcal{A}_k(k)$ but no element of order p^{m+1} lifts. To make it possible we need $\mathcal{O}_K^\times((1+\pi_L\mathcal{O}_L)^{p^{m+1}}+\mathfrak{m}\mathcal{O}_L)$ to be a proper subgroup of $\mathcal{O}_K^\times((1+\pi_L\mathcal{O}_L)^{p^m} + \mathfrak{m}\mathcal{O}_L)$. But for a non-negative integer ℓ we have

$$(1+\pi_L\mathcal{O}_L)^{p^\ell} + \pi_K\mathcal{O}_L \subseteq 1 + \pi_L^{p^\ell}\mathcal{O}_L + \pi_L^d\mathcal{O}_L$$

so this is the case if L/K is sufficiently ramified such that $d > p^m$.

Remark 2.3.7. Let A/K be an abelian variety with non-Archimedean uniformization

$$0 \to \Lambda \to G \to A \to 0.$$

By [LL01, Proposition 6.1 (a)], if A/K has split reduction then G/K has split reduction. We can use our construction to show that the converse is not true. The non-Archimedean uniformization of the Tate curve E/L associated to $q \in L^\times$ is given by the exact sequence of rigid analytic groups

$$0 \to q^{\mathbb{Z}} \to \mathbb{G}_{m,L} \to E \to 0.$$

Then, the non-Archimedean uniformization of $A = \operatorname{Res}_{L/K} E/K$ is given by

$$0 \to \operatorname{Res}_{L/K} q^{\mathbb{Z}} \to \operatorname{Res}_{L/K} \mathbb{G}_{m,L} \to \operatorname{Res}_{L/K} E \to 0.$$

It follows from Proposition 2.3.1 that

$$\Phi(\operatorname{Res}_{L/K} \mathbb{G}_{m,L}) \cong \Phi(\mathbb{G}_{m,L}),$$

so in particular $\Phi(\operatorname{Res}_{L/K} \mathbb{G}_{m,L})$ is free. This implies that $\operatorname{Res}_{L/K} \mathbb{G}_{m,L}$ has split reduction but as we saw A/K may not have split reduction.

Remark 2.3.8. By [LL01, Proposition 1.11], if G/K and G'/K are semi-abelian varieties and $f : G \to G'$ is an isogeny of degree prime to p then G/K has split reduction if and only if G'/K has split reduction. We can use our construction to give an explicit example of two isogenous abelian varieties, one which has split reduction and the other one which does not have split reduction. This shows that [LL01, Proposition 1.11] is not true for isogenies of degree divisible by p.

Let $p > 2$. Let $K = \mathbb{Q}_p^{\mathrm{ur}}$ be the maximal unramified extension of the field of p-adic numbers and let $L = \mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)$ where ζ_p is a p-th root of 1. We have $d = [L : K] = p - 1$. Let $q = \pi_L^p$ and $q' = \zeta_p q$ and let E/L and E'/L be the Tate curves associated to q and q'. These two elliptic curves are isogenous to the Tate curve over L associated to $q^p = q'^p$ by raising to the power p

$$\mathbb{G}_{m,L}/q^{\mathbb{Z}} \xrightarrow{(\ )^p} \mathbb{G}_{m,L}/q^{p\mathbb{Z}} \xleftarrow{(\ )^p} \mathbb{G}_{m,L}/q'^{\mathbb{Z}}.$$

Therefore E/L and E'/L are isogenous. As the Weil restriction of an isogeny is an isogeny, $\mathrm{Res}_{L/K}\, E/K$ and $\mathrm{Res}_{L/K}\, E'/K$ are isogenous. But now

$$q/\pi_L^p = 1 \in (1 + \pi_L \mathcal{O}_L)^p + \pi_K \mathcal{O}_L$$

whereas

$$q'/\pi_L^p = \zeta_p \notin (1 + \pi_L \mathcal{O}_L)^p + \pi_K \mathcal{O}_L$$

because $v_L(\zeta_p - 1) = v_L(p)/(p-1) = 1$ but $(1 + \pi_L\mathcal{O}_L)^p + \pi_K\mathcal{O}_L = 1 + \pi_L^{p-1}\mathcal{O}_L$. Hence, by Corollary 2.3.3, $\mathrm{Res}_{L/K}\, E/K$ has split reduction but $\mathrm{Res}_{L/K}\, E'/K$ does not have split reduction.

2.4 Splitting properties and the Weil restriction

Our construction in Section 2.3 leads to the question of the relation between the Weil restriction and splitting properties of semi-abelian varieties. A first answer is given in [LL01, Remark 3.10]. The authors give an example of an elliptic curve which have split reduction but whose Weil restriction does not have split reduction. Using Corollary 2.3.3 we get other examples of this kind since Tate curves have semi-abelian reduction and thus have split reduction. In this section we want to study the general situation.

2.4.1 Reduction of Weil restrictions

Let K be a complete discrete valuation field with ring of integers $\mathcal{O}_K$ and uniformizing element π_K. Let G/K be a semi-abelian variety with Néron model $\mathcal{G}/\mathcal{O}_K$. For any positive integer n we denote by

$$\mathcal{G}_n = \mathcal{G} \times_{\mathcal{O}_K} \mathcal{O}_K/\pi_K^n\mathcal{O}_K$$

the infinitesimal fiber, by

$$r_n : G(K) \to \mathcal{G}_n(\mathcal{O}_K/\pi_K^n\mathcal{O}_K)$$

the reduction map and by $G^n(K)$ the kernel of this reduction map.

Proposition 2.4.1. *Let L/K be a finite separable extension and let G/L be a semi-abelian variety. We have the following implications :*

(1) if $\operatorname{Res}_{L/K} G/K$ has split reduction then G/L has split reduction;

(2) if G/L has totally not split reduction then $\operatorname{Res}_{L/K} G/K$ has totally not split reduction.

Proof. Let us compute $(\operatorname{Res}_{L/K} G)^1(K)$. Using the base change formula (2.4) we find that this is the kernel of the reduction map

$$(\operatorname{Res}_{L/K} G)(K) \to (\operatorname{Res}_{(\mathcal{O}_L/\pi_K\mathcal{O}_L)/k}(\mathcal{G} \times_{\mathcal{O}_L} \mathcal{O}_L/\pi_K\mathcal{O}_L))(k),$$

i.e. of the reduction map

$$r_d : G(L) \to \mathcal{G}_d(\mathcal{O}_L/\pi_L^d\mathcal{O}_L)$$

where $d = [L : K]$. Hence, we have $(\operatorname{Res}_{L/K} G)^1(K) = G^d(L) \subseteq G^1(L)$.

Let us show assertion (1). Let us suppose that $\operatorname{Res}_{L/K} G/K$ has split reduction. Let $\varphi \in \Phi(G) \cong \Phi(\operatorname{Res}_{L/K} G)$ (by Proposition 2.3.1) be an element of finite order n. Then φ lifts to an element $x \in (\operatorname{Res}_{L/K} G)(K) = G(L)$ such that $n \cdot x \in (\operatorname{Res}_{L/K} G)^1(K) \subseteq G^1(L)$. Thus, G/L has split reduction.

Assertion (2) follows from a similar argument. □

In the remaining part of this section we will give a recipe to build counterexamples to the reciprocal of assertions (1) and (2) based on the case by case study in [LL01, Section 2].

2.4.2 Reduction of elliptic curves

Let L be a complete discrete valuation field with valuation v_L, ring of integers $\mathcal{O}_L$ and uniformizing element π_L. Let E/L be an elliptic curve. Let $\mathcal{E}/\mathcal{O}_L$ be its Néron model. Assume that E/L is given by a minimal Weierstrass equation

$$y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathcal{O}_L$ for $i \in \{1, 2, 3, 4, 6\}$. When $a_i \in \pi_L\mathcal{O}_L$ for all $i \in \{1, 2, 3, 4, 6\}$ then the reduced equation has a singular point at $(0, 0)$. Let $E^0(L)$ denote the set of rational points in $E(L)$ whose reduction modulo π_L is not $(0, 0)$. Equivalently $E^0(L) \cong \mathcal{E}^0(\mathcal{O}_L)$ under the isomorphism $E(L) \cong \mathcal{E}(\mathcal{O}_L)$ (see [Sil94, Corollary IV.9.2]) and thus we have

$$\Phi(E) \cong E(L)/E^0(L).$$

For any positive integer n the subgroup $E^n(L) \subseteq E^0(L)$ defined in §2.4.1 is given by

$$E^n(L) = \{P \in E(L) \mid x(P)/y(P) \in \pi_L^n\mathcal{O}_L\}.$$

We will denote by $z = -x/y$ the parameter at ∞.

2.4.3 A key point

Let us recall an important fact from [LL01, Section 2]. Assume that E/L has additive reduction. Let $P, Q \in E(L)$ be two points whose reductions in $\mathcal{E}_k(k)$ are lying in the same non-trivial component. Then, the orders of those reductions in $\mathcal{E}_k(k)$ are equal. This is only due to the fact that the identity component of the special fiber is killed by p and so it applies more generally in this context. In particular, given a field K as in the introduction such that L is a finite extension of K, it applies to $\mathrm{Res}_{L/K} E/K$. Indeed,

$$(\mathrm{Res}_{\mathcal{O}_L/\mathcal{O}_K} \mathcal{E})^0_k \cong \mathrm{Res}_{(\mathcal{O}_L/\pi_K\mathcal{O}_L)/k} \mathbb{G}_{a,(\mathcal{O}_L/\pi_K\mathcal{O}_L)}$$

by Proposition 2.3.1 and the base change formula (2.4) and thus

$$(\mathrm{Res}_{\mathcal{O}_L/\mathcal{O}_K} \mathcal{E})^0_k(k) \cong \mathcal{O}_L/\pi_K\mathcal{O}_L$$

which is killed by p. Note that $(\mathrm{Res}_{\mathcal{O}_L/\mathcal{O}_K} \mathcal{E})^0_k$ is a unipotent algebraic group over k.

2.4.4 First example

Let us follow [LL01, §2.13]. Let $p = 3$. Let E/L be of type **IV**. Then, we have $\Phi(E) \cong \mathbb{Z}/3\mathbb{Z}$. It is shown that we may assume $a_1 = a_3 = 0$ and that we have the following inequalities for the valuations of the coefficients

a_2	a_4	a_6	b_2	b_4	b_6	b_8
≥ 1	≥ 2	2	≥ 1	≥ 2	2	≥ 3

with the relations $b_2 = 4a_2$, $b_4 = 2a_4$, $b_6 = 4a_6$ and $b_8 = 4a_2a_6 - a_4^2$. As we mentioned in §2.4.3, to study the splitting properties of E/L or $\mathrm{Res}_{L/K} E/K$ it is enough to consider one point with non-trivial image in $\Phi(E) \cong \Phi(\mathrm{Res}_{L/K} E)$. Let $P = (0, y(P))$ with $y(P)^2 = a_6$ which is clearly not in $E^0(L)$. Assume that P is not of 3-torsion. We use the formulas in [Sil86, III.2.3] to compute $v_L(z(3P))$.

We have

$$\begin{aligned}
x(2P) &= -\frac{b_8}{b_6}, \\
y(2P) &= -\frac{a_4 x(2P)}{2y(P)} - \frac{a_6}{y(P)}, \\
x(3P) &= \left(\frac{y(2P) - y(P)}{x(2P)}\right)^2 - a_2 - x(2P), \\
y(3P) &= -\left(\frac{y(2P) - y(P)}{x(2P)}\right) x(3P) - y(P).
\end{aligned}$$

Thus,

$$x(3P) = \frac{1}{x(2P)^2}\left(\frac{a_4 x(2P) + 4a_6}{2y(P)}\right)^2 - a_2 - x(2P)$$

and by considering the valuations we get

$$v_L(x(3P)) = 6 - 2v_L(b_8) \leq 0.$$

Then, we have

$$y(3P) = \frac{1}{x(2P)}\left(\frac{a_4 x(2P) + 4a_6}{2y(P)}\right) x(3P) - y(P)$$

and by considering the valuations we have

$$v_L(y(3P)) = 3 - v_L(b_8) + v_L(x(3P)).$$

Hence, we find that

$$v_L(z(3P)) = v_L(b_8) - 3 \geq 0.$$

By definition E/L does not have split reduction if and only if $3P \notin E^1(L)$. We recover here that this is equivalent to $v_L(b_8) = 3$. Set $m = v_L(b_8) - 3$. If $m > 0$ then E/L has split reduction but for a subextension L/K of degree $d > m$, if such an extension exists, $3P \notin E^d(L) = (\operatorname{Res}_{L/K} E)^1(L)$, i.e. $\operatorname{Res}_{L/K} E$ does not have split reduction. Whence, the reciprocal to Proposition 2.4.1 (1) is false.

2.4.5 Second example

Let us follow [LL01, §2.6]. Let $p = 2$. Let E/L be of type $\mathbf{I}_0^*$. We have $\Phi(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is shown that we can find three points

$$P_i = (\pi_L \alpha_i, 0) \in E(L),$$

with $\alpha_i \in \mathcal{O}_L$ for $i \in \{1, 2, 3\}$ whose reductions modulo π_L are distinct, such that their images in $\Phi(E)$ are the three distinct non-trivial points. More precisely, we have

$$x^3 + a_2 x^2 + a_4 x + a_6 = (x - \pi_L \alpha_1)(x - \pi_L \alpha_2)(x - \pi_L \alpha_3).$$

We have the following inequalities for the valuations of the coefficients

a_1	a_2	a_3	a_4	a_6	b_2	b_4	b_6	b_8
≥ 1	≥ 1	≥ 2	≥ 2	≥ 3	≥ 2	≥ 3	≥ 4	≥ 4

We will compute $v_L(z(2P_i))$ for $i \in \{1, 2, 3\}$ and P_i's that are not of 2-torsion.

Let us write $x_i = \pi_L \alpha_i$ for $i \in \{1,2,3\}$. Without loss of generality we may do the computation taking $i = 1$. Recall that we have

$$x(2P) = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6}.$$

Moreover $x^4 - b_4x^2 - 2b_6x - b_8$ is congruent to $(x^2 - a_4)^2$ modulo π^4 and $a_4 = \pi^2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$. Now $x_1^2 - a_4 = \pi^2(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)$ and thus the valuation of the numerator of $x(2P_1)$ is 4. As in [LL01, §2.6], the valuation of the denominator of $x(2P_1)$ is $2v_L(a_1x_1 + a_3)$ and so we have

$$v_L(x(2P_1)) = 4 - 2v_L(a_1x_1 + a_3) \leq 0.$$

Then, we have

$$y(2P_1) = -(\lambda + a_1)x(2P_1) - \nu - a_3$$

where

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4}{a_1x_1 + a_3}$$

and

$$\nu = \frac{-x_1^3 + a_4x_1 + 2a_6}{a_1x_1 + a_3}.$$

Now, we get

$$\begin{aligned} -(a_1x_1 + a_3)y(2P_1) = (3x_1^2 &+ 2a_2x_1 + a_4 + a_1(a_1x_1 + a_3))x(2P_1) \\ &- x_1^3 + a_4x_1 + 2a_6 + a_3(a_1x_1 + a_3). \end{aligned}$$

Using that $3x^2 + a_4$ have valuation 4 we find that

$$v_L(y(2P)) = 2 + v_L(x(2P)) - v_L(a_1x + a_3).$$

Hence, for $i \in \{1,2,3\}$ we have

$$v_L(z(2P_i)) = v_L(a_1x_i + a_3) - 2 \geq 0.$$

Let $m_i = v_L(a_1x_i + a_3) - 2$ for $i \in \{1,2,3\}$. Assume that E does not have totally not split reduction so that $m_i > 0$ for some i. Then, for a subextension L/K of degree sufficiently large, $\mathrm{Res}_{L/K} E$ has totally not split reduction. Whence, the reciprocal to Proposition 2.4.1 (2) is false.

2.5 Split reduction of Jacobian varieties after a tamely ramified extension

Let K be a complete discrete valuation field with ring of integers $\mathcal{O}_K$ and algebraically closed residue field k of characteristic exponent p. Let K^s be a fixed separable closure of K. Let G/K be a semi-abelian variety of dimension g. Let $\mathcal{G}/\mathcal{O}_K$ be its Néron model with special fiber $\mathcal{G}_k/k$.

2.5.1 Edixhoven's filtration

In the case where G/K is abelian, Edixhoven defined a filtration on $\mathcal{G}_k/k$ by closed subgroups (see [Edi92]). It was extended to semi-abelian varieties by Halle and Nicaise in [HN11]. Let us recall the construction of this filtration, following [HN16, §5.1.3]. For every positive integer d prime to p, let $K(d)/K$ be the unique degree d extension of K in K^s and let $\mathcal{O}_{K(d)}$ be the ring of integers of $K(d)$. Since $K(d)/K$ is tamely ramified, it is Galois. Let us denote by Γ the Galois group $\mathrm{Gal}(K(d)/K)$ and by $\mathcal{G}(d)/\mathcal{O}_{K(d)}$ the Néron model of $G_{K(d)} = G \times_K K(d)$. Let

$$\mathcal{W} = \mathrm{Res}_{\mathcal{O}_{K(d)}/\mathcal{O}_K} \mathcal{G}(d)$$

be the Weil restriction of $\mathcal{G}(d)/\mathcal{O}_{K(d)}$ under the extension $\mathcal{O}_{K(d)}/\mathcal{O}_K$. Then, Γ acts on $\mathcal{W}/\mathcal{O}_K$ and the fixed locus $\mathcal{W}^\Gamma/\mathcal{O}_K$ is canonically isomorphic to $\mathcal{G}/\mathcal{O}_K$ (see [Edi92, Theorem 4.2] or [HN11, Proposition 4.1]). Let $\pi_{K(d)}$ be a uniformizing element of $K(d)$. For every $i \in \{0, \dots, d\}$, the reduction modulo $\pi^i_{K(d)}$ defines a morphism of group schemes

$$(\mathcal{W}^\Gamma)_k = (\mathcal{W}_k)^\Gamma \to \mathrm{Res}_{(\mathcal{O}_{K(d)}/\pi^i_{K(d)}\mathcal{O}_{K(d)})/k}(\mathcal{G}(d) \times_{\mathcal{O}_{K(d)}} \mathcal{O}_{K(d)}/\pi^i_{K(d)}\mathcal{O}_{K(d)})$$

whose kernel is denoted by $F^i_d\mathcal{G}_k$. We get a filtration

$$\mathcal{G}_k = F^0_d\mathcal{G}_k \supset F^1_d\mathcal{G}_k \supset \cdots \supset F^d_d\mathcal{G}_k = 0$$

on $\mathcal{G}_k/k$ by closed subgroups, and $F^i_d\mathcal{G}_k/k$ is a smooth and connected unipotent algebraic group for all $i > 0$. Let us denote by

$$\mathrm{Gr}^i_d \mathcal{G}_k = F^i_d\mathcal{G}_k/F^{i+1}_d\mathcal{G}_k$$

the graded quotients of this filtration. We say that $j \in \{0, \dots, d-1\}$ is a $K(d)$-*jump of* G/K if $\dim(\mathrm{Gr}^j_d \mathcal{G}_k) > 0$ and we call this dimension the *multiplicity of* j.

Edixhoven also introduced a filtration on $\mathcal{G}_k/k$ by rational indices that captures the filtrations introduced above simultaneously for all d. For every rational number $\alpha = a/b$ in $\mathbb{Z}_{(p)} \cap [0, 1[$, with a, b nonnegative integers and b prime to p, we put

$$\mathcal{F}^\alpha\mathcal{G}_k = F^a_b\mathcal{G}_k.$$

By [HN11, Lemma 4.11], this definition does not depend on the choice of a and b and we get a filtration $\mathcal{F}^\bullet\mathcal{G}_k$ of $\mathcal{G}_k/k$ by closed subgroups. Note that there are only finitely many closed subgroups occuring in the filtration $\mathcal{F}^\bullet\mathcal{G}_k$ because $\mathcal{G}_k/k$ is Noetherian. Let ρ be an element of $\mathbb{R} \cap [0, 1[$. Set $\mathcal{F}^{>\rho}\mathcal{G}_k = \mathcal{F}^\beta\mathcal{G}_k$, where β is any value in $\mathbb{Z}_{(p)} \cap]\rho, 1[$ such that $\mathcal{F}^{\beta'}\mathcal{G}_k = \mathcal{F}^\beta\mathcal{G}_k$ for all $\beta' \in \mathbb{Z}_{(p)} \cap]\rho, \beta]$. If $\rho \neq 0$, set $\mathcal{F}^{<\rho}\mathcal{G}_k = \mathcal{F}^{\gamma}\mathcal{G}_k$, where γ is any value in $\mathbb{Z}_{(p)} \cap [0, \rho[$ such that $\mathcal{F}^{\gamma'}\mathcal{G}_k = \mathcal{F}^{\gamma}\mathcal{G}_k$ for all $\gamma' \in \mathbb{Z}_{(p)} \cap [\gamma, \rho[$. Set $\mathcal{F}^{<0}\mathcal{G}_k = \mathcal{G}_k$. Then, let us define

$$\mathrm{Gr}^{\rho}\, \mathcal{G}_k = \mathcal{F}^{<\rho}\mathcal{G}_k / \mathcal{F}^{>\rho}\mathcal{G}_k$$

for every $\rho \in \mathbb{R} \cap [0, 1[$. We say that $j \in \mathbb{R} \cap [0, 1[$ is a *jump of* G/K if $\dim(\mathrm{Gr}^j\, \mathcal{G}_k) > 0$ and we call this dimension the *multiplicity of* j. Counted with multiplicities, G/K has exactly g jumps.

2.5.2 The case of Jacobian varieties

Let C/K be a smooth, proper and geometrically connected curve of genus $g > 0$. Assume that C/K has a divisor of degree one. Let the *stabilization index* of C/K (see [HN16, Definition 3.2.2.3]) be the least common multiple of the multiplicities of the principal components (i.e. components of positive genus or intersecting the other components in at least three points) in the special fiber of the minimal model with strict normal crossings of C over $\mathcal{O}_K$. Let us denote the stabilization index of C/K by $e(C/K)$. Let L be the minimal finite separable extension of K in K^s such that $C \times_K L$ has semistable reduction. If this extension is tamely ramified then $e(C/K) = [L : K]$ (see [HN16, Proposition 3.2.2.4]) but this is false in general.

Proposition 2.5.1. *Let $J = \mathrm{Jac}(C)/K$ be the Jacobian variety of C/K and let $\mathcal{J}/\mathcal{O}_K$ be its Néron model. Let U/k be the unipotent part of $\mathcal{J}^0_k/k$. Let d be a positive integer prime to p. If $d > e(C/K)$ then U/k is the kernel of the canonical morphism*

$$\mathcal{J}_k \to \mathcal{J}(d)_k.$$

Proof. Let u be the dimension of U. By [EHN15, Proposition 5.4.3], u is equal to the number of nonzero jumps of J/K counted with multiplicities. Hence $\mathcal{F}^{>0}\mathcal{J}_k$ is a connected unipotent subgroup of $\mathcal{J}_k$ of dimension u. This implies that $\mathcal{F}^{>0}\mathcal{J}_k = U$. By [HN16, Corollary 5.3.1.5], the jumps of J/K are rational numbers and the stabilization index $e(C/K)$ is their least common denominator. This implies that the smallest nonzero jump of J/K is $\geq 1/e(C/K)$. Then, $1/d < 1/e(C/K)$ implies that $\mathcal{F}^{>0}\mathcal{J}_k = \mathcal{F}^{1/d}\mathcal{J}_k$. Thus, we get

$$U = \mathcal{F}^{>0}\mathcal{J}_k = \mathcal{F}^{1/d}\mathcal{J}_k = F^1_d\mathcal{J}_k.$$

Now, the fact that U/k is the kernel of the canonical morphism

$$\mathcal{J}_k \to \mathcal{J}(d)_k$$

follows from the definition of the filtration $F^{\bullet}_d\mathcal{J}_k$ (see [Edi92, Remark 6.4.6]). $\square$

Theorem 2.5.2. *Let $J = \mathrm{Jac}(C)/K$ be the Jacobian variety of C/K. Let d be a positive integer prime to p. If $d > e(C/K)$, then $J_{K(d)}/K(d)$ has split reduction.*

Proof. First, let $a = \gcd(e(C/K), d)$. Then $K(d)/K(a)$ is a tamely ramified extension of degree d/a. Let $C(a) = C \times_K K(a)$. By [HN16, Corollary 3.2.2.10], the stabilization index of $C(a)/K(a)$ is given by

$$e(C(a), K(a)) = e(C/K)/a.$$

Hence, we have $d/a > e(C(a), K(a))$. Let $\mathcal{J}/\mathcal{O}_K$ be the Néron model of J/K. The previous proposition applied to $C(a)/K(a)$ implies that the unipotent part U/k of $\mathcal{J}(a)^0_k/k$ is the kernel of the canonical morphism

$$\mathcal{J}(a)_k \to \mathcal{J}(d)_k.$$

Now, by [HN16, Proposition 1.3.3.1], we have $|\Phi(J_{K(d)})| = (d/a)^{t_{K(a)}}|\Phi(J_{K(a)})|$, where $t_{K(a)}$ is the dimension of the toric part of $\mathcal{J}(a)^0_k$. As d/a is prime to p, the orders of $\Phi(J_{K(a)})_p$ and $\Phi(J_{K(d)})_p$ are the same. Moreover, by [ELL96, Theorem 1], the kernel of the canonical morphism

$$\Phi(J_{K(a)}) \to \Phi(J_{K(d)})$$

is killed by d/a which is prime to p. Hence, this morphism is an isomorphism on the p-primary parts of these groups.

Finally, we can proceed as in the proof of [LL01, Proposition 3.3]. Let $\varphi' \in \Phi(J_{K(d)})$ be an element of order p^r where $r > 0$. Let $\varphi \in \Phi(J_{K(a)})$ be the corresponding element under the above morphism and let $x \in \mathcal{J}(a)_k$ be in the preimage of φ. Let x' be the image of x in $\mathcal{J}(d)_k$. As in the proof of [LL01, Propositin 1.4 (b)], we may assume that $p^r \cdot x \in U$. Thus, we have $p^r \cdot x' = 0$. Since x' is in the preimage of φ', this proves that $J_{K(d)}/K(d)$ has split reduction. □

Remark 2.5.3. In Proposition 2.5.1 and Theorem 2.5.2 we need to assume that the abelian variety is the Jacobian variety of a curve of index one to be able to use [EHN15, Proposition 5.4.3], [HN16, Corollary 5.3.1.5] and [HN16, Proposition 1.3.3.1]. If one can prove these results without this hypothesis then Theorem 2.5.2 would be true for arbitrary semi-abelian varieties over K provided that we have a suitable definition of the stabilization index $e(G/K)$ of arbitrary semi-abelian varieties G/K. This problem is discussed in [HN16, Part 4, §1].

Corollary 2.5.4. *Let $J = \mathrm{Jac}(C)/K$ be the Jacobian variety of C/K. There exists a constant c depending on g only such that if M/K is any tamely ramified extension of degree $> c$, then J_M/M has split reduction.*

Proof. All we need to prove is that if $g > 0$ is fixed, then the stabilization index of a curve C/K of genus g is bounded by a constant c. This follows from Corollaire 1.4.15 for $g \geq 2$ and from Kodaira-Néron classification for elliptic curves. □

Remark 2.5.5. In the case of elliptic curves, one checks that the stabilization index is at most 6. Hence, we almost recover Theorem 2.2.8 (3) which states that M/K of degree ≥ 4 is enough to acquire split reduction.

Finally, let us remark that in the case of elliptic curves we have the following alternative result to Theorem 2.5.2.

Proposition 2.5.6. *Let E/K be an elliptic curve. Let L/K be the minimal finite separable extension such that E_L/L has semi-abelian reduction. Let d be a positive integer prime to p. If $d > [L : K]$, then $E_{K(d)}/K(d)$ has split reduction.*

Proof. By Theorem 2.2.8 (c), if $d \geq 4$ then $E_{K(d)}/K(d)$ has split reduction. Hence, the only case to tackle is then $[L : K] = 2$ and $d = 3$. In this case, the reduction type cannot be **IV** or **IV*** because for these types the groups of components are of order 3 and should be killed by $[L : K]$ by [ELL96, Theorem 1]. If E/K has reduction type $\mathbf{I}_n^*$ then $e(E/K) = 2$ and the result follows from Theorem 2.5.2. Thus, we may assume that the reduction type of E/K is either **II**, **III**, **III*** or **II***. Recall that we have the following formula for Swan conductors

$$\delta(E_{K(d)}/K(d)) = d \cdot \delta(E/K).$$

By [LL01, Lemma 3.4], the reduction type of $E_{K(d)}/K(d)$ will be either **II**, **III**, **III***, **II*** or $\mathbf{I}_0^*$. By Theorem 2.2.8 (a), in order that $E_{K(d)}/K(d)$ does not have split reduction we must have $\delta(E/K) = 1$. Let Δ be the minimal discriminant of E/K. Then, Ogg's formula implies that $v_K(\Delta) \in \{3, 4, 10, 11\}$. But this is not possible if $[L : K] = 2$. Hence, $E_{K(d)}/K(d)$ has split reduction. □

2.6 Splitting properties and the Swan conductor

2.6.1 Swan conductor of Weil restrictions

Let L/K be a finite separable extension. Let E/L be an elliptic curve and let $A = \mathrm{Res}_{L/K}\, E/K$ be its Weil restriction under the extension L/K. By [Mil72, §1, Lemma], the Swan conductor of A/K is given by the following formula

$$\delta(A/K) = \delta(E/L) + 2(v_L(\mathcal{D}_{L/K}) - (p-1)), \tag{2.7}$$

where $\mathcal{D}_{L/K}$ is the different ideal of the extension L/K. Before tackling Question 2.2.10 let us start with some preliminary results.

2.6.2 Some preliminaries

Let L be a complete discrete valuation field with algebraically closed residue field. Let E/L be an elliptic curve which acquires multiplicative reduction over a quadratic separable extension M/L. Then, there exists $q \in L^\times$ such that E/L is isomorphic over M to the Tate curve defined by q (see [Sil94, Theorem V.5.3]). Hence, the non-Archimedean uniformization of E/L is given by the following exact sequence

$$0 \to \Lambda \to \mathrm{Res}^1_{M/L}\,\mathbb{G}_{m,M} \to E \to 0,$$

where $\mathrm{Res}^1_{M/L}\,\mathbb{G}_{m,M}$ is the norm torus defined in §2.2.6 and Λ/L is the lattice

$$\mathrm{Res}_{M/L}\, q^{\mathbb{Z}} \cap \mathrm{Res}^1_{M/L}\,\mathbb{G}_{m,M},$$

where $q^{\mathbb{Z}}/M$ is the constant lattice in $\mathbb{G}_{m,M}/M$.

Lemma 2.6.1. *Keep the previous notation. Assume that $v_L(q)$ is odd. Then, the following assertions are equivalent :*

1. *E/L has totally not split reduction;*
2. *E/L does not have split reduction;*
3. *$\mathrm{Res}^1_{M/L}\,\mathbb{G}_{m,M}/L$ has totally not split reduction;*
4. *$\mathrm{Res}^1_{M/L}\,\mathbb{G}_{m,M}/L$ does not have split reduction.*

Proof. As $v_L(q)$ is odd, the group of components $\Phi(E)$ is cyclic (see [Lor10, Theorem 2.8]). Thus, (1) $\Leftrightarrow$ (2) follows from [LL01, Proposition 1.4(e)]. Then, (3) $\Leftrightarrow$ (4) is trivial since $\Phi(\mathrm{Res}^1_{M/L}\,\mathbb{G}_{m,M}) \cong \mathbb{Z}/2\mathbb{Z}$ by [LL01, Proposition 4.17 (2)]. Now, the lemma follows from by [LL01, Proposition 6.1 (a) and (b)]. □

Proposition 2.6.2. *Let L/K be a quadratic separable extension and let σ be the non-trivial element of* $\mathrm{Gal}(L/K)$. *Let E/L be an elliptic curve which acquires multiplicative reduction over a quadratic separable extension M/L. Let $q \in L^\times$ be such that E_M/M is isomorphic to the Tate curve defined by q. If $q/\sigma(q)$ is not a root of* 1 *then the abelian variety $A = \mathrm{Res}_{L/K} E/K$ is simple.*

Proof. We have $\dim(A) = 2$ (see §2.3.2). Let B/K be an abelian variety of dimension 1 and assume that there is a non-trivial K-morphism

$$B \to A.$$

Then, by property of the Weil restriction we get an L-isogeny

$$B \times_K L \to E.$$

From this, we get another L-isogeny

$$B \times_K L \to {}^{\sigma}E.$$

Hence, E and ${}^{\sigma}E$ should be L-isogenous. Now, the elliptic curve ${}^{\sigma}E/L$ is isomorphic over M to the Tate curve defined by $\sigma(q) \in L^{\times}$. If $q/\sigma(q)$ is not a root of 1, then q and $\sigma(q)$ are not commensurable, i.e. there are no non-zero integers m, n such that $q^n = \sigma(q)^m$. By [Tat97, §Isogenies, Theorem], this implies that E and ${}^{\sigma}E$ are not isogenous over M hence neither over L. Whence, A/K is simple. □

2.6.3 Counterexample to Question 2.2.10

Assume that K is of residue characteristic 2. Let L/K be a quadratic separable extension. It follows from [LL01, Lemmata 4.1(b) and 4.5] and Theorem 2.2.9 (1) that one can choose a quadratic separable extension M/L such that $\mathrm{Res}^1_{M/L}\,\mathbb{G}_{m,M}$ does not have split reduction. Let σ be the non-trivial element of $\mathrm{Gal}(L/K)$. Let us choose $q \in L^{\times}$ with $v_L(q)$ odd and such that $q/\sigma(q)$ is not a root of 1. Consider the elliptic curve E/L given by the uniformization in §2.6.2. It follows from Lemma 2.6.1 that E/L has totally not split reduction. Then, by Proposition 2.4.1, $A = \mathrm{Res}_{L/K}\,E/K$ has totally not split reduction. Finally, it follows from Proposition 2.6.2 that A/K is simple. We already mentionned in §2.4.3 that

$$\mathcal{A}^0_k = \mathrm{Res}_{(\mathcal{O}_L/\pi_K\mathcal{O}_L)/k}\,\mathbb{G}_{a,(\mathcal{O}_L/\pi_K\mathcal{O}_L)}$$

is a unipotent algebraic group over k and thus the toric rank of A/K is 0. Now we have

$$1 \leq \delta(E/L) \leq 3$$

by Theorem 2.2.8 (1) and thus it is clear from Formula (2.7) that $\delta(A/K)$ really depends on the field K. Whence, the answer to Question 2.2.10 is negative even for simple abelian varieties over K.

To conclude, let us give a concrete example. Let $\mathbb{Q}_2^{ur}$ be the maximal unramified extension of the field of 2-adic numbers. Let $d \geq 2$ be an integer. Let $K = \mathbb{Q}_2^{ur}(\pi_K)$ with $\pi_K^d = 2$ and let $L = K(\pi_L)$ with $\pi_L^2 = \pi_K$. The different ideal of L/K is $2\pi_L\mathcal{O}_L$ (use [Ser68, Corollaire III.6.2]). Let $q = \pi_L^n(1 + \pi_L)$ with n odd. Let σ be the non-trivial element of $\mathrm{Gal}(L/K)$. We have

$$q/\sigma(q) = -(1 + \pi_L)/(1 - \pi_L),$$

and this is not a root of 1 because it is not in $\mathbb{Q}_2^{ur}$ (apply σ). Now, let M/L be the extension defined by the Eisenstein polynomial $t^2 + \pi_L t + \pi_L$. The different ideal of the extension M/L is $\mathcal{D}_{M/L} = \pi_L \mathcal{O}_M$ (use [Ser68, Corollaire III.6.2]). Then, by [LL01, Lemmata A.1 (b) and 4.5] we have

$$\begin{aligned} \delta(\mathrm{Res}^1_{M/L}\, \mathbb{G}_{m,M}/L) &= v_M(\mathcal{D}_{M/L}) - (2-1) \\ &= 1. \end{aligned}$$

It follows from Theorem 2.2.9 (1) that $\mathrm{Res}^1_{M/L}\, \mathbb{G}_{m,M}$ has totally not split reduction. Now, by [LL01, Proposition 6.4 (b)], we have

$$\begin{aligned} \delta(E/L) &= 2\delta(\mathrm{Res}^1_{M/L}\, \mathbb{G}_{m,M}/L) \\ &= 2. \end{aligned}$$

Finally, by formula (2.7), we have

$$\begin{aligned} \delta(A/K) &= \delta(E/L) + 2(v_L(2\pi_L) - (2-1)) \\ &= 2 + 4d. \end{aligned}$$

Remark 2.6.3. As suggested in [LL01], one may ask the same question for the more restricted class of abelian varieties such that the representation of the absolute Galois group $\mathrm{Gal}(K^s/K)$ on the Tate module $T_\ell(A)$, $\ell \neq p$, is irreducible. We do not know any counterexample of this kind.

2.6.4 Brumer and Kramer's bound

Before tackling Question 2.2.11, let us recall the bound for the Swan conductor given in [BK94]. For any abelian variety A/K and any extension M/K, let us denote by a_M and t_M the dimensions of the abelian and toric parts of the reduction of A_M/M respectively. Let us consider the following function on integers

$$\lambda_p(n) = \sum_{i=0}^{s} i r_i p^i,$$

where

$$n = \sum_{i=0}^{s} r_i p^i$$

is the p-adic expansion of n, with $0 \leq r_i < p$.

Proposition 2.6.4. *[BK94, Proposition 3.11]*

Assume that K is of characteristic 0. Let A/K be an abelian variety which acquires semi-abelian reduction over L. Let K_1 be the subfield of L fixed by the first ramification subgroup of $\mathrm{Gal}(L/K)$. We have

$$\delta(A/K) \leq 2(d_t + d_a)pv_K(p) + (p-1)(2\lambda_p(d_t) + \lambda_p(2d_a))v_K(p),$$

where d_t and d_a are defined by $t_L - t_{K_1} = (p-1)d_t$ and $a_L - a_{K_1} = (p-1)d_a$ respectively.

2.6.5 Counterexample to Question 2.2.11

Assume that K is of characteristic 0 and that it contains the p-th roots of 1. Let L/K be the Kummer extension given by the polynomial $t^p - \pi_K$. Let E/L be an elliptic curve and let $A = \mathrm{Res}_{L/K} E/K$ be its Weil restriction under the extension L/K. Using [Ser68, Corollaire III.6.2] we can compute $\mathcal{D}_{L/K} = p\pi_L^{p-1}\mathcal{O}_L$ and then formula (2.7) gives

$$\begin{aligned} \delta(A/K) &= \delta(E/L) + 2v_L(p) \\ &= \delta(E/L) + 2pv_K(p). \end{aligned}$$

Assume that E/L is a Tate curve. Then E/L has semi-abelian reduction and thus $\delta(E/L) = 0$ so that $\delta(A/K) = 2pv_K(p)$. Now let us compute the bound for the Swan conductor from Proposition 2.6.4. Here, the Galois group $\mathrm{Gal}(L/K)$ coincides with the first ramification subgroup, hence the subfield of L fixed by the latter is simply K. By Proposition 2.3.5, A_L/L has purely multiplicative reduction. Thus, we have $a_K = a_L = 0$ hence $d_a = 0$ and $t_K = 1$ (see the exact sequence (2.5)) whereas $t_L = p$ hence $d_t = 1$. We also have $\lambda_p(0) = \lambda_p(1) = 0$ and therefore we get

$$\delta(A/K) \leq 2pv_K(p).$$

This bound is exactly the one we achieved. Now we saw in Proposition 2.3.3 that we may choose our elliptic curve E/L such that A/K does not have split reduction and therefore the answer to Question 2.2.11 is no in general.

Remark 2.6.5. Our example has positive toric rank ($t_K = 1$). We do not know any example of abelian variety with toric rank 0 which does not have split reduction and whose conductor achieves the bound from [BK94].

Remark 2.6.6. Assume that K is of characteristic $p > 0$. Let L/K be the extension given by the Eisenstein polynomial $t^p + a_{p-1}t + a_p$ where $a_{p-1} \in \pi_K\mathcal{O}_K$ is different from 0 and $v_K(a_p) = 1$. This polynomial is separable and the different ideal of the extension L/K is $\mathcal{D}_{L/K} = a_{p-1}\mathcal{O}_L$ (use [Ser68, Corollaire III.6.2]). Now, let E/L be an elliptic curve with totally not split reduction. Let $A = \mathrm{Res}_{L/K} E$ be its Weil restriction under the extension L/K. Then, A/K has totally not split reduction by Proposition 2.4.1. Moreover, by formula (2.7) we have

$$\delta(A/K) = \delta(E/L) + 2pv_K(a_{p-1}) - (p-1).$$

Hence, considering an unbounded family of a_{p-1}'s we get a family of abelian varieties which have totally not split reduction but unbounded Swan conductors.

Chapitre 3

Modèles de Néron et groupes formels

Soit $\mathcal{O}_K$ un anneau de valuation discrète complet. Soit K le corps des fractions de $\mathcal{O}_K$ de caractéristique 0. Soient π_K une uniformisante de K et $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$ le corps résiduel de $\mathcal{O}_K$ de caractéristique $p > 0$. Soit A/K une variété abélienne de dimension g. Un théorème de Mattuck établit l'existence d'un voisinage π_K-adique de l'origine 0 dans $A(K)$ isomorphe au polydisque $(\pi_K\mathcal{O}_K)^g$ muni de sa structure de groupe additif usuelle. On s'intéresse à préciser le rayon de ce voisinage de 0. Tout d'abord, on montre que l'obstruction à l'isomorphisme souhaité est la torsion dans le noyau de la réduction de A/K qui est un groupe formel sur $\mathcal{O}_K$. Ensuite, on étudie l'effet d'un changement de base sur ce groupe formel. Enfin, on détermine la valeur du rayon recherché dans le cas des courbes elliptiques.

3.1 Un théorème de Mattuck

3.1.1 Le noyau de la réduction

Soit A/K une variété abélienne de dimension g. Soit $\mathcal{A}/\mathcal{O}_K$ son modèle de Néron. Pour un entier $n \geq 1$, on définit la fibre infinitésimale

$$\mathcal{A}_n = \mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_K/\pi_K^n\mathcal{O}_K,$$

l'application de réduction

$$r_n : A(K) \to \mathcal{A}_n(\mathcal{O}_K/\pi_K^n\mathcal{O}_K),$$

et on note $A_n(K)$ le noyau de cette application.

Proposition 3.1.1. *Le noyau de la réduction $A_1(K)$ est le groupe associé à un groupe formel commutatif de dimension g.*

Démonstration. Soit 0 l'élément neutre de la fibre spéciale $\mathcal{A}_k/k$. Soit $\mathcal{O}_{\mathcal{A},0}$ l'anneau local de $\mathcal{A}/\mathcal{O}_K$ en 0. On démontre tout d'abord que l'on a une bijection

$$A_1(K) \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathrm{Spec}\,\mathcal{O}_K, \mathrm{Spec}\,\mathcal{O}_{\mathcal{A},0}) \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_{\mathcal{A},0}, \mathcal{O}_K).$$

Soit $P \in A_1(K)$. Par la propriété de Néron, P s'étend en une section

$$\mathrm{Spec}\,\mathcal{O}_K \to \mathcal{A}$$

qui se factorise par

$$\mathrm{Spec}\,\mathcal{O}_{\mathcal{A},0} \to \mathcal{A}$$

d'où un morphisme

$$\mathrm{Spec}\,\mathcal{O}_K \to \mathrm{Spec}\,\mathcal{O}_{\mathcal{A},0}.$$

Réciproquement, la fibre générique d'un morphisme

$$\mathrm{Spec}\,\mathcal{O}_K \to \mathrm{Spec}\,\mathcal{O}_{\mathcal{A},0}$$

définit un point $P \in A_1(K)$.

Soit $\hat{\mathcal{O}}_{\mathcal{A},0}$ le complété de l'anneau local $\mathcal{O}_{\mathcal{A},0}$ pour la topologie $\mathfrak{m}$-adique où $\mathfrak{m}$ est l'idéal maximal de $\mathcal{O}_{\mathcal{A},0}$. Comme $\mathcal{O}_K$ est complet, on a d'après la propriété universelle de la complétion une bijection

$$A_1(K) \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_{\mathcal{A},0}, \mathcal{O}_K) \cong \mathrm{Hom}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathcal{A},0}, \mathcal{O}_K).$$

Comme $\mathcal{A}/\mathcal{O}_K$ est lisse en 0, on a un isomorphisme

$$\hat{\mathcal{O}}_{\mathcal{A},0} \cong \mathcal{O}_K[[X_1, \ldots, X_g]].$$

Ainsi, on peut identifier $A_1(K)$ avec $(\pi_K \mathcal{O}_K)^g$.

De plus, la loi de groupe $\mathcal{A} \times_{\mathcal{O}_K} \mathcal{A} \to \mathcal{A}$ induit en localisant en 0 puis en complétant pour la topologie $\mathfrak{m}$-adique un morphisme

$$\mathcal{O}_K[[X_1, \ldots, X_g]] \to \mathcal{O}_K[[Y_1, \ldots, Y_g, Z_1, \ldots, Z_g]].$$

On note F_i l'image de X_i par ce morphisme. Le g-uplet de séries formelles F obtenu forme un groupe formel commutatif. En effet, les axiomes d'associativité et de commutativité sont une conséquence des mêmes axiomes pour la loi de groupe sur $\mathcal{A}/\mathcal{O}_K$. Quant au fait que pour tout $i \in \{1, \ldots, g\}$ on ait

$$F_i(X, Y) = Y_i + Z_i + (\text{termes de degré } \geq 2),$$

cela vient du fait que la différentielle de la loi de groupe est donnée par

$$\begin{array}{ccc} T_{\mathcal{A},0} \times T_{\mathcal{A},0} & \to & T_{\mathcal{A},0} \\ (Y, Z) & \mapsto & Y + Z. \end{array}$$

Ainsi, on a un isomorphisme $A_1(K) \cong F(\pi_K \mathcal{O}_K)$. $\square$

Soit v_K la valuation sur K normalisée de sorte que $v_K(\pi_K) = 1$. On note $A(K)'_{\text{tors}}$ l'ensemble des points de torsion de $A(K)$ d'ordre premier à p.

Corollaire 3.1.2. *On a les propriétés suivantes :*

(1) $A(K)'_{\text{tors}}$ *s'injecte dans* $\mathcal{A}_k(k)$.

(2) Si $v_K(p) < p - 1$ *alors* $A(K)_{\text{tors}}$ *s'injecte dans* $\mathcal{A}_k(k)$.

Démonstration. Le point (1) est une conséquence de la proposition 1.7.19 qui assure qu'il n'y a pas de point de torsion d'ordre premier à p dans le groupe formel $A_1(K)$. Le point (2) est une conséquence du point (1) et du Théorème 1.7.21 qui assure qu'il n'y a pas de point de torsion d'ordre p dans $A_1(K)$ dès que $v_K(p) < p - 1$. □

Dans le cas général, $A_1(K)$ peut contenir des éléments de torsion.

3.1.2 Le logarithme formel

D'après la proposition 3.1.1, on a un isomorphisme

$$A_1(K) \cong F(\pi_K \mathcal{O}_K),$$

où F est un groupe formel commutatif sur $\mathcal{O}_K$ de dimension g. D'après 1.7.13, on dispose d'un logarithme formel

$$\log_F : F(X, Y) \to \hat{\mathbb{G}}_a^g(X, Y)$$

qui induit un isomorphisme local

$$\log_F : A_1(K) \to (\pi_K \mathcal{O}_K)^g$$

où l'ensemble de droite est muni de sa loi de groupe additif usuelle.

Proposition 3.1.3. *Le noyau du morphisme*

$$\log_F : A_1(K) \to (\pi_K \mathcal{O}_K)^g$$

est le sous-groupe de torsion $A_1(K)_{\text{tors}}$.

Démonstration. Comme $(\pi_K \mathcal{O}_K)^g$ est sans torsion, l'inclusion $A_1(K)_{\text{tors}} \subseteq \ker \log_F$ est claire. Réciproquement, soit $x \in \ker \log_F$. D'après le lemme 1.7.11

$$[p]_F\,(X) = pX + (\text{termes de degré } \geq 2).$$

Ainsi, pour n assez grand $[p^n]_F\,(x)$ est dans l'ouvert où $\log_F$ est un isomorphisme. Ainsi $[p^n]_F\,(x) = 0$, i.e. $x \in A_1(K)_{\text{tors}}$. □

L'image du morphisme ci-dessus peut être décrite via la proposition suivante.

Proposition 3.1.4. *Un sous-groupe ouvert connexe d'un polydisque* $(\pi_K \mathcal{O}_K)^g$ *est analytiquement isomorphe à un polydisque.*

Démonstration. C'est un cas particulier de [Lut16, Proposition 7.2.3]. □

On peut maintenant démontrer le théorème suivant qui est dû à Arthur Mattuck (voir [Mat55, Theorem 7]).

Théorème 3.1.5. *Pour tout entier* $n > v_K(p)/(p-1)$, $A_n(K)$ *est analytiquement isomorphe au polydisque* $(\pi_K \mathcal{O}_K)^g$ *muni de sa structure de groupe additif usuelle.*

Démonstration. On conserve les notations utilisées ci-dessus. D'après 1.7.21, pour $n > v_K(p)/(p-1)$ alors $A_n(K) \cong F(\pi_K^n \mathcal{O}_K)$ est sans torsion. Ainsi d'après la proposition 3.1.3, $A_n(K)$ est isomorphe à son image dans $(\pi_K \mathcal{O}_K)^g$ par le logarithme $\log_F$ qui est un polydisque d'après la proposition précédente. □

Corollaire 3.1.6. *On suppose que* k *est fini. Alors,* $A(K)$ *contient un sous-groupe d'indice fini isomorphe à* $\mathcal{O}_K^g$.

Démonstration. On a une suite exacte

$$0 \to A_1(K) \to A(K) \to \mathcal{A}_k(k).$$

Comme k est un corps fini, $\mathcal{A}_k(k)$ est fini et on est donc ramené à montrer que $A_1(K)$ contient un sous-groupe d'indice fini isomorphe à $\mathcal{O}_K^g$.

On a un isomorphisme $A_1(K) \cong F(\pi_K \mathcal{O}_K)$ où F est un groupe formel commutatif sur $\mathcal{O}_K$ de dimension g. Soit $n > v_K(p)/(p-1)$. D'après le théorème précédente on a un isomorphisme

$$F(\pi_K^n \mathcal{O}_K) \cong \mathcal{O}_K^g.$$

Ainsi, il suffit de montrer que $F(\pi_K^n \mathcal{O}_K)$ est d'indice fini dans $F(\pi_K \mathcal{O}_K)$.

Soit $i \in \{1, \ldots, n-1\}$. L'identité

$$F(X, Y) = X + Y + (\text{termes de degré } \geq 2)$$

implique que l'application

$$F(\pi_K^i \mathcal{O}_K)/F(\pi_K^{i+1} \mathcal{O}_K) \to \pi_K^i \mathcal{O}_K / \pi_K^{i+1} \mathcal{O}_K$$

induite par l'identité sur les ensembles est un isomorphisme. Ainsi, on a une filtration

$$F(\pi_K^n \mathcal{O}_K) \subseteq F(\pi_K^{n-1} \mathcal{O}_K) \subseteq \cdots \subseteq F(\pi_K \mathcal{O}_K)$$

dont les quotients successifs sont finis, d'où le résultat. □

Remarque 3.1.7. En particulier, si k est fini alors on obtient que $A(K)_{\text{tors}}$ est fini.

3.1.3 Heuristique

On s'intéresse dans la suite de ce chapitre à la question suivante.

Question 3.1.8. *Quel est le plus petit entier n tel que $A_n(K)$ soit analytiquement isomorphe au polydisque $(\pi_K \mathcal{O}_K)^g$ muni de sa structure de groupe additif usuelle ?*

On a vu que l'obstruction pour l'application $\log_F$ à être un isomorphisme est liée au groupe $A_1(K)_{\mathrm{tors}}$ dont les éléments sont d'ordre une puissance de p. On illustre maintenant pourquoi le type de réduction de A/K doit avoir une influence sur la réponse à apporter à la question précédente. Pour simplifier, on suppose ici que k est algébriquement clos.

En considérant la p-torsion dans la suite exacte

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi(A) \to 0$$

on obtient une suite exacte

$$0 \to \mathcal{A}_k^0[p] \to \mathcal{A}_k[p] \to \Phi(A)[p] \to \mathcal{A}_k^0/p\mathcal{A}_k^0 \to \cdots .$$

On considère les trois différents cas suivants.

(1) Si A/K a bonne réduction, $\mathcal{A}_k/k$ est une variété abélienne et on a alors

$$\mathcal{A}_k[p](k) \cong (\mathbb{Z}/p\mathbb{Z})^h$$

où $0 \leq h \leq g$ est le p-rang de $\mathcal{A}_k/k$. Or $A[p](K)$ peut avoir jusqu'à p^{2g} points auquel cas l'application de réduction

$$A[p](K) \to \mathcal{A}_k[p](k)$$

ne peut pas être injective. Dans ce cas $A_1(K)_{\mathrm{tors}}$ n'est pas trivial et donc $A_1(K)$ n'est pas isomorphe à $(\pi_K \mathcal{O}_K)^g$ i.e. $n = 1$ ne convient pas.

(2) Si A/K a réduction purement multiplicative, $\mathcal{A}_k^0 \cong \mathbb{G}_m^g$ et alors $\mathcal{A}_k^0[p] = 0$ et $\mathcal{A}_k^0/p\mathcal{A}_k^0 = 0$ puisque la multiplication par p est surjective sur $\mathbb{G}_m^g$. Ainsi, la suite exacte ci-dessus donne un isomorphisme

$$\mathcal{A}_k[p] \cong \Phi(A)[p],$$

or on sait que

$$\Phi(A)[p] \cong (\mathbb{Z}/p\mathbb{Z})^h$$

avec $0 \leq h \leq g$. Comme $A[p](K)$ peut avoir encore une fois jusqu'à p^{2g} points on obtient comme précédemment que $n = 1$ ne convient pas.

(3) Si A/K a réduction purement additive, alors $\mathcal{A}_k^0(k)$ peut avoir beaucoup de points et on ne peut pas exclure que l'application

$$A[p](K) \to \mathcal{A}_k[p](k)$$

soit injective, i.e. que $n = 1$ convienne.

3.2 Groupes formels et changement de base

Soit L/K une extension finie. Soit $\mathcal{O}_L$ l'anneau des entiers de L. Soit $\mathcal{A}'/\mathcal{O}_L$ le modèle de Néron de $A_L = A \times_K L$. On notera 0 les éléments neutres des fibres spéciales $\mathcal{A}_k$ ou $\mathcal{A}'_k$ sans distinction. Par la propriété de Néron, on a un morphisme

$$h : \mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{A}'.$$

On en déduit un morphisme injectif

$$\hat{\mathcal{O}}_{\mathcal{A}',0} \hookrightarrow \hat{\mathcal{O}}_{\mathcal{A}\times_{\mathcal{O}_K}\mathcal{O}_L,0}.$$

Soit π_L une uniformisante de L. Soient $x_1, \dots, x_g$ et $y_1, \dots, y_g$ des systèmes de coordonnées locales en 0 de $\mathcal{A}/\mathcal{O}_K$ et $\mathcal{A}'/\mathcal{O}_L$ respectivement. On a alors

$$\hat{\mathcal{O}}_{\mathcal{A}\times_{\mathcal{O}_K}\mathcal{O}_L,0} \cong \mathcal{O}_L[[x_1, \dots, x_g]]$$

et

$$\hat{\mathcal{O}}_{\mathcal{A}',0} \cong \mathcal{O}_L[[y_1, \dots, y_g]].$$

D'où un morphisme injectif

$$\mathcal{O}_L[[y_1, \dots, y_g]] \hookrightarrow \mathcal{O}_L[[x_1, \dots, x_g]].$$

Proposition 3.2.1. *Il existe un choix de systèmes de coordonnées locales en* 0 *de* $\mathcal{A}$ *et* $\mathcal{A}'$ *tel que*

$$\begin{array}{rcl} y_1 & = & \pi_L^{r_1} x_1 \\ & \vdots & \\ y_g & = & \pi_L^{r_g} x_g \end{array}$$

où $r_1, \dots, r_g$ *sont des entiers naturels.*

Démonstration. On considère le morphisme induit par h entre les faisceaux des différentielles relatives

$$h^*\Omega^1_{\mathcal{A}'/\mathcal{O}_L} \to \Omega^1_{\mathcal{A}\times_{\mathcal{O}_K}\mathcal{O}_L/\mathcal{O}_K}.$$

En tirant en arrière par la section unité de $\mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_L$ on obtient un morphisme entre les $\mathcal{O}_L$-modules libres des différentielles invariantes

$$\omega_{\mathcal{A}'/\mathcal{O}_L} \to \omega_{\mathcal{A}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} \mathcal{O}_L.$$

Ce morphisme est injectif puisque c'est un isomorphisme à la fibre générique.

D'après le théorème de la base adaptée, il existe alors une base

$$\mathrm{d}x_1, \dots, \mathrm{d}x_g$$

de $\omega_{\mathcal{A}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} \mathcal{O}_L$ (qui provient d'une base sur $\mathcal{O}_K$ à un automorphisme $\mathcal{O}_L$-linéaire près) telle que pour un certain g-uplet d'entiers naturels $r_1, \dots, r_g$ la famille

$$\pi_L^{r_1} \mathrm{d}x_1, \dots, \pi_L^{r_g} \mathrm{d}x_g$$

soit une base de $\omega_{\mathcal{A}'/\mathcal{O}_L}$.

Il reste à démontrer que l'on obtient de cette manière un système de coordonnées locales de $\mathcal{A}/\mathcal{O}_K$ en 0. On considère

$$x_1, \dots, x_g \in \mathcal{O}_{\mathcal{A},0}$$

tels que la famille

$$\mathrm{d}x_1, \dots, \mathrm{d}x_g \in \omega_{\mathcal{A}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} \mathcal{O}_L$$

soit la base obtenue ci-dessus. Quitte à remplacer x_i par $x_i - x_i(0)$ on peut supposer que $x_i \in \mathfrak{m}_{\mathcal{A},0}$ pour $i \in \{1, \dots, g\}$. On définit alors un morphisme

$$\varphi : U \to \mathbb{A}^g_{\mathcal{O}_K}$$

où U est un voisinage ouvert de 0 dans $\mathcal{A}$, via

$$\begin{array}{rcl} \mathcal{O}_K[T_1, \dots, T_g] & \to & \Gamma(U, \mathcal{O}_{\mathcal{A}}) \\ T_i & \mapsto & x_i. \end{array}$$

On a, par construction, un isomorphisme

$$(\varphi^* \Omega^1_{\mathbb{A}^g_{\mathcal{O}_K}/\mathcal{O}_K})_0 \cong (\Omega^1_{U/\mathcal{O}_K})_0.$$

Ainsi, φ est un morphisme étale en 0 d'après [Liu02, Proposition 6.2.10]. Comme les corps résiduels en 0 sont isomorphes cela implique que

$$\begin{array}{rcl} \mathcal{O}_K[[T_1, \dots, T_g]] & \to & \hat{\mathcal{O}}_{\mathcal{A},0} \\ T_i & \mapsto & x_i \end{array}$$

est un isomorphisme d'après [Liu02, Proposition 4.3.26], ce qu'il fallait démontrer.

Enfin, en posant $y_i = \pi_L^{r_i} x_i$ pour $i \in \{1, \dots, g\}$ on obtient un système de coordonnées locales de $\mathcal{A}'/\mathcal{O}_L$ en 0 tel que

$$\begin{array}{rcl} \hat{\mathcal{O}}_{\mathcal{A}',0} & \to & \hat{\mathcal{O}}_{\mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_L, 0} \\ y_i & \mapsto & \pi_L^{r_i} x_i. \end{array}$$

D'où la proposition. $\square$

Soit $e(L/K)$ l'indice de ramification de l'extension L/K. Dans [Cha00] et [CY01], Chai et Yu ont introduit la notion de conducteur de changement de base pour les tores et les variétés abéliennes. On considère le morphisme injectif induit par h sur les algèbres de Lie

$$\mathrm{Lie}(h) : \mathrm{Lie}(\mathcal{A}) \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \mathrm{Lie}(\mathcal{A}').$$

Le conoyau de ce morphisme est de longueur finie. Si L/K est une extension finie telle que A_L/L ait réduction semi-abélienne, alors le *conducteur de changement de base* de A/K est défini par

$$c(A) = \frac{1}{e(L/K)} \ell_{O_L} \,\mathrm{Coker}(\mathrm{Lie}(h)).$$

Le module $\omega_{\mathcal{A}/\mathcal{O}_K}$ étant le dual de $\mathrm{Lie}(\mathcal{A})$, la longueur du conoyau de $\mathrm{Lie}(h)$ est égale à la longueur du conoyau du morphisme

$$\omega_{\mathcal{A}'/\mathcal{O}_L} \to \omega_{\mathcal{A}/\mathcal{O}_K} \otimes_{\mathcal{O}_K} \mathcal{O}_L.$$

On obtient ainsi l'égalité

$$c(A) = \frac{r_1 + r_2 + \cdots + r_g}{e(L/K)},$$

avec les notations de la proposition précédente.

3.3 Le cas des courbes elliptiques

Soit E/K une courbe elliptique. Soit $\mathcal{E}/\mathcal{O}_K$ son modèle de Néron. D'après la proposition 3.1.1, il existe un groupe formel commutatif F sur $\mathcal{O}_K$ tel que le noyau de la réduction $E_1(K)$ soit isomorphe à $F(\pi_K \mathcal{O}_K)$. On s'intéresse à déterminer le plus petit entier n tel que $E_n(K)$ soit analytiquement isomorphe au disque $\pi_K \mathcal{O}_K$ muni de sa structure de groupe additif usuelle. D'après la proposition 3.1.3, il suffit de choisir n strictement plus grand que la valuation maximale d'un point non trivial de $E_1(K)_{\mathrm{tors}}$. D'après la proposition 1.7.19, un élément de $E_1(K)_{\mathrm{tors}}$ est d'ordre une puissance de p, on va donc considérer le morphisme de multiplication par p sur le groupe formel F de E/K. On remarque que le fait que

$$[p]_F(X) = pX + (\text{termes de degré } \geq 2)$$

implique que

$$v_K([p]_F(\zeta)) > v_K(\zeta).$$

Ainsi, si $\zeta \in E_1(K)_{\mathrm{tors}}$ est d'ordre p^k avec $k \geq 2$, alors $[p^{k-1}]_F(\zeta)$ est d'ordre p et

$$v_K([p^{k-1}]_F(\zeta)) > v_K(\zeta).$$

Il suffit donc de calculer la valuation maximale des points de $E_1(K)_{\mathrm{tors}}$ d'ordre p.

3.3.1 Réduction semi-abélienne

Dans le cas où E/K a réduction semi-abélienne, i.e. bonne réduction ou réduction multiplicative, on peut calculer la valuation des zéros non triviaux de $[p]_F(X)$ à l'aide du polygone de Newton de cette série formelle.

Proposition 3.3.1. *Soit E/K une courbe elliptique.*

(1) Si E/K a réduction multiplicative ou bonne réduction ordinaire, alors la valuation des points de $E_1(K)_{\mathrm{tors}}$ d'ordre p est

$$\frac{v_K(p)}{(p-1)}.$$

(2) Si E/K a bonne réduction supersingulière, on note e_1 la valuation du coefficient s_p de X^p dans $[p]_F(X)$.

(a) Si $e_1 \geq pv_K(p)/(p+1)$, alors la valuation des points de $E_1(K)_{\mathrm{tors}}$ d'ordre p est

$$\frac{v_K(p)}{(p^2-1)}.$$

(b) Si $e_1 < pv_K(p)/(p+1)$, alors la valuation maximale des points de $E_1(K)_{\mathrm{tors}}$ d'ordre p est

$$\frac{v_K(p)-e_1}{p-1}.$$

Démonstration. On suit [Ser72, §1.10]. Dans le cas (1), la loi de groupe formel F est de hauteur 1 et le polygone de Newton de $[p]_F(X)$ est composé d'un unique segment de pente

$$\frac{v_K(p)}{(p-1)}.$$

Dans le cas (2), la loi de groupe formel F est de hauteur 2. Suivant la valeur de e_1, le polygone de Newton de $[p]_F(X)$ est formé d'un unique segment de pente

$$\frac{v_K(p)}{p^2-1},$$

ou de deux segments de pentes

$$\frac{v_K(p)-e_1}{p-1}$$

et

$$\frac{v_K(p)}{p^2-p} < \frac{v_K(p)-e_1}{p-1}.$$

D'où le résultat d'après la théorie des polygones de Newton. □

Remarque 3.3.2. Soit $\mathcal{H}(E,\omega)$ l'*invariant de Hasse* comme défini dans [Kat73, §2.0]. On a la congruence

$$s_p \equiv \mathcal{H}(E,\omega) \bmod p\mathcal{O}_K.$$

Remarque 3.3.3. Pour $p > 3$, on peut exprimer $e_1 = v_K(s_p)$ en fonction uniquement de la classe de p modulo 12 et des valuations du discriminant minimal Δ et du j-invariant $j(E)$ de E/K (voir [Loz13, Theorem 3.9]).

3.3.2 Réduction additive

Étant donnée une courbe elliptique E/K, il existe toujours une extension finie L/K telle que E_L/L a réduction semi-abélienne. On se ramène ainsi aux valeurs ci-dessus via la proposition suivante. On notera π_L une uniformisante de L et v_L la valuation sur L normalisée par $v_L(\pi_L) = 1$.

Proposition 3.3.4. *Soit E/K une courbe elliptique. Soit L/K une extension finie telle que E_L/L a réduction semi-abélienne. Soit v la valuation maximale des points d'ordre p du noyau de la réduction de E_L/L. Alors, la valuation maximale des points de $E_1(K)_{\mathrm{tors}}$ d'ordre p est*

$$\frac{v}{e(L/K)} - c(E)$$

où $c(E)$ est le conducteur de changement de base de E/K.

Démonstration. Soit $\mathcal{E}'/\mathcal{O}_L$ le modèle de Néron de E_L/L. D'après la proposition 3.2.1, on peut trouver des paramètres locaux z et z' en 0 de $\mathcal{E}/\mathcal{O}_K$ et $\mathcal{E}'/\mathcal{O}_L$ respectivement tel que via le morphisme injectif

$$\hat{\mathcal{O}}_{\mathcal{E}',0} \cong \mathcal{O}_L[[z']] \to \hat{\mathcal{O}}_{\mathcal{E}\times_{\mathcal{O}_K}\mathcal{O}_L,0} \cong \mathcal{O}_L[[z]]$$

on ait

$$z' = \pi_L^r z$$

où r est un entier naturel. Par définition, $r = e(L/K)c(E)$ où $c(E)$ est le conducteur de changement de base de E/K.

On note F' la loi de groupe formel de $\mathcal{E}'/\mathcal{O}_L$. On a le diagramme commutatif suivant

$$\begin{tikzcd}
(\mathcal{E}\times_{\mathcal{O}_K}\mathcal{O}_L)\times_{\mathcal{O}_L}(\mathcal{E}\times_{\mathcal{O}_K}\mathcal{O}_L) \arrow[r] \arrow[d] & \mathcal{E}'\times_{\mathcal{O}_L}\mathcal{E}' \arrow[d] \\
\mathcal{E}\times_{\mathcal{O}_K}\mathcal{O}_L \arrow[r] & \mathcal{E}'
\end{tikzcd},$$

où les flèches verticales sont les lois de groupe. En localisant en 0 et en complétant, on obtient un diagramme commutatif

$$\begin{array}{ccc} \mathcal{O}_L[[z_1, z_2]] & \leftarrow & \mathcal{O}_L[[z'_1, z'_2]] \\ \uparrow & & \uparrow \\ \mathcal{O}_L[[z]] & \leftarrow & \mathcal{O}_L[[z']] \end{array}.$$

En suivant l'image de z', on a alors la relation

$$\pi_L^r F(z_1, z_2) = F'(\pi_L^r z_1, \pi_L^r z_2)$$

et donc

$$\pi_L^r [p]_F(z) = [p]_{F'}(\pi_L^r z).$$

Soit $\zeta \in \pi_K \mathcal{O}_K$ tel que $[p]_F(\zeta) = 0$. Alors $[p]_{F'}(\pi_L^r \zeta) = 0$ et d'après la proposition 3.3.1 on connaît $v = v_L(\pi_L^r \zeta)$. On obtient donc

$$v_K(\zeta) = \frac{v}{e(L/K)} - c(E).$$

D'où la proposition. □

Remarque 3.3.5. D'après [HN16, proposition 2.2.1], on a

$$c(E) = \begin{cases} v_K(\Delta)/12 & \text{si } j(E) \in \mathcal{O}_K, \\ (v_K(\Delta) + v_K(j(E)))/12 & \text{si } j(E) \notin \mathcal{O}_K. \end{cases}$$

Remarque 3.3.6. La borne de la proposition 3.3.4 dépend uniquement de E/K et non de l'extension L/K. En effet, si on est potentiellement dans le cas (1) de la proposition 3.3.1, on obtient

$$\frac{v_L(p)}{e(L/K)(p-1)} - c(E) = \frac{v_K(p)}{p-1} - c(E).$$

Si on est potentiellement dans le cas (2)(a), on obtient

$$\frac{v_L(p)}{e(L/K)(p^2-1)} - c(E) = \frac{v_K(p)}{p^2-1} - c(E).$$

Finalement, si on est potentiellement dans le cas (2)(b), on obtient

$$v = \frac{v_L(p) - e'_1}{p-1}$$

où e'_1 est la valuation sur L du coefficient s'_p de z'^p dans $[p]_{F'}(z')$. Mais, d'après la démonstration précédente, on a

$$\pi_L^r [p]_F(z) = [p]_{F'}(\pi_L^r z),$$

et donc $\pi_L^r s_p = \pi_L^{rp} s_p'$. D'où $e_1'/e(L/K) = e_1 - (p-1)c(E)$, et ainsi on obtient

$$\frac{v}{e(L/K)} - c(E) = \frac{v_K(p) - e_1}{p-1}.$$

Pour conclure, le plus petit entier n tel que $E_n(K)$ soit analytiquement isomorphe au disque $\pi_K \mathcal{O}_K$ muni de sa structure de groupe additif usuelle est le plus petit entier n strictement supérieur à la valeur obtenue dans les propositions 3.3.1 et 3.3.4 suivant le type de réduction de E/K. Cela répond à la question 3.1.8 dans le cas des courbes elliptiques et précise donc le théorème de Mattuck dans ce cas.

Chapitre 4

Modèles de groupes algébriques de dimension 1

Soit K un corps de valuation discrète complet de caractéristique 0. Soit $\mathcal{O}_K$ l'anneau des entiers de K. Soit π_K une uniformisante de K. Soit $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$ le corps résiduel de $\mathcal{O}_K$ supposé algébriquement clos sauf mention contraire. Tout d'abord, on rappelle la définition d'ensemble de points de Néron d'un groupe algébrique suivant [Fal08]. Ensuite, on s'intéresse aux modèles sur $\mathcal{O}_K$ des groupes additif et multiplicatif $\mathbb{G}_{a,K}/K$ et $\mathbb{G}_{m,K}/K$ et plus particulièrement à leurs groupes des composantes. Enfin, dans le cas d'un corps résiduel fini, on s'intéresse aux points rationnels des groupes des composantes de tels modèles.

4.1 Points de Néron et modèles associés

Faltings a introduit la notion de point de Néron dans [Fal08] dans le but d'assouplir la définition de modèle de Néron habituelle.

Définition 4.1.1. Soit X/K un schéma. On appelle *point de Néron* de X/K un élément de $X(K')$ où K' est le corps des fractions d'un anneau de valuation discrète $\mathcal{O}_{K'}$ formellement lisse sur $\mathcal{O}_K$ (i.e. π_K est toujours une uniformisante de $\mathcal{O}_{K'}$ et le corps résiduel $\mathcal{O}_{K'}/\pi_K\mathcal{O}_{K'}$ est une extension de type fini séparable, mais non nécessairement algébrique, de k).

On notera que le corps K' dépend du point de Néron $P \in X(K')$ que l'on considère. On donne maintenant les définitions d'ensemble de points de Néron ouvert et borné, toujours en suivant [Fal08].

Définition 4.1.2. On dira qu'un ensemble $\mathcal{E}$ de points de Néron est *ouvert* s'il existe un schéma lisse $\mathcal{S}/\mathcal{O}_K$ avec $\mathcal{S}_k \neq \emptyset$ et un morphisme lisse et dominant

$$\varphi : \mathcal{S}_K \to X$$

tel que la réduction des éléments de $\mathcal{E}$ qui se relèvent en des éléments de $\mathcal{S}(\mathcal{O}_{K'})$ (i.e. $P \in X(K')$ est l'image par φ de la fibre générique d'une section $\operatorname{Spec} \mathcal{O}_{K'} \to \mathcal{S}$) est Zariski-dense dans $\mathcal{S}_k/k$.

Définition 4.1.3. On dira que $\mathcal{E}$ est *borné* s'il existe un schéma $\mathcal{Y}/\mathcal{O}_K$ de type fini et un morphisme

$$\mathcal{Y}_K \to X$$

tel que tous les éléments de $\mathcal{E}$ se relèvent en des éléments de $\mathcal{Y}(\mathcal{O}_{K'})$.

Soit G/K un groupe algébrique de type fini. Soit $\mathcal{E}$ un ensemble de point de Néron ouvert, borné et stable par produit et inverse (pour définir le produit de deux points de Néron qui ne sont pas définis sur le même corps il est nécessaire de définir la notion de changement de base d'un point de Néron, on renvoie à [Fal08, page 94]). On a alors le résultat suivant.

Théorème 4.1.4. *[Fal08, Theorem 1]*
Il existe un unique schéma lisse, de type fini et séparé $\mathcal{G}/\mathcal{O}_K$ qui étend G/K tel que

(1) tout élément $P \in G(K')$ de $\mathcal{E}$ s'étend en un élément de $\mathcal{G}(\mathcal{O}_{K'})$,

(2) la réduction de ces points est Zariski-dense dans la fibre spéciale $\mathcal{G}_k/k$.
De plus, si $\mathcal{S}/\mathcal{O}_K$ est un schéma lisse muni d'un morphisme $\mathcal{S}_K \to G$ tel que les éléments de $\mathcal{E}$ qui se relèvent en des éléments de $\mathcal{S}(\mathcal{O}_{K'})$ ont une réduction Zariski-dense dans la fibre spéciale $\mathcal{S}_k/k$, alors le morphisme $\mathcal{S}_K \to G$ s'étend en un morphisme $\mathcal{S} \to \mathcal{G}$.

On dira que $\mathcal{G}/\mathcal{O}_K$ est le *modèle de Néron de G/K associé à l'ensemble de points de Néron $\mathcal{E}$*.

Remarque 4.1.5. Tout schéma en groupes $\mathcal{G}/\mathcal{O}_K$ lisse, de type fini et séparé est le modèle de Néron de sa fibre générique $\mathcal{G}_K/K$ associé à l'ensemble de points de Néron $\mathcal{E}$ formé par l'image du morphisme canonique $\mathcal{G}(\mathcal{O}_K) \to \mathcal{G}_K(K)$.

Ceci nous amène à étudier quels peuvent être les modèles lisses, de type fini et séparés sur $\mathcal{O}_K$ d'un groupe algébrique de type fini G/K. On s'intéressera plus particulièrement aux cas où G/K est le groupe additif $\mathbb{G}_{a,K}/K$ ou le groupe multiplicatif $\mathbb{G}_{m,K}/K$. L'étude de ces modèles a déjà été menée dans [DW74] et [WW80], où des équations sont données. On déterminera ici quelles sont les possibilités pour le groupe des composantes d'un tel modèle et on donnera un procédé géométrique permettant d'obtenir tous les cas possibles. Enfin, on rappelle que d'après [SGA3, Corollaire 12.10.1], si $\mathcal{G}/\mathcal{O}_K$ est un schéma en groupes plat, séparé et de type fini tel que $\mathcal{G}_K/K$ est affine, alors $\mathcal{G}$ est affine. Ainsi, les modèles recherchés ici seront affines.

Soit G/K un groupe algébrique de type fini. Soit $\mathcal{G}/\mathcal{O}_K$ un modèle lisse, de type fini et séparé de G/K. On notera $\mathcal{G}^0/\mathcal{O}_K$ la composante connexe de 0 dans $\mathcal{G}/\mathcal{O}_K$ et $\pi_0(\mathcal{G}_k)$ le groupe des composantes de la fibre spéciale $\mathcal{G}_k/k$.

4.2 Modèles du groupe additif

Soit $\mathcal{G}/\mathcal{O}_K$ un modèle affine et lisse de $\mathbb{G}_{a,K}/K$.

4.2.1 Caractéristique résiduelle nulle

Proposition 4.2.1. *On suppose que k est de caractéristique 0. Alors, $\mathcal{G}_k/k$ est connexe et on a*

$$\mathcal{G} \cong \mathbb{G}_{a,\mathcal{O}_K}.$$

Démonstration. On a une suite exacte

$$0 \to \mathcal{G}_k^0 \to \mathcal{G}_k \to \pi_0(\mathcal{G}_k) \to 0.$$

Comme la multiplication par un entier n quelconque est surjective sur le groupe algébrique $\mathcal{G}_k^0/k$, on obtient en passant aux points de n-torsion la suite exacte

$$0 \to \mathcal{G}_k^0[n] \to \mathcal{G}_k[n] \to \pi_0(\mathcal{G}_k)[n] \to 0.$$

Si $\pi_0(\mathcal{G}_k)$ n'est pas trivial, alors, pour un certain entier n, $\mathcal{G}_k[n]$ n'est pas trivial. Comme $\mathcal{O}_K$ est hensélien et $\mathcal{G}[n]/\mathcal{O}_K$ est (étale donc) quasi-fini, on a une décomposition en somme disjointe $\mathcal{G}[n] = \mathcal{G}[n]^f \amalg \mathcal{G}[n]'$ où $\mathcal{G}[n]^f$ est fini étale sur $\mathcal{O}_K$ et $\mathcal{G}[n]'$ est un K-schéma. De plus, $\mathcal{G}[n]^f$ est un sous-schéma en groupes de $\mathcal{G}[n]$. En utilisant encore le fait que $\mathcal{O}_K$ est hensélien, on a $\mathcal{G}[n](k) = \mathcal{G}[n]^f(k) \cong \mathcal{G}[n]^f(K)$, d'où une injection $\mathcal{G}_k(k)[n] \hookrightarrow \mathcal{G}_K(K)[n]$. Comme $\mathcal{G}_K(K)[n]$ est trivial, on a une contradiction. Ainsi, $\pi_0(\mathcal{G}_k)$ est trivial, i.e. $\mathcal{G}_k/k$ est connexe.

On a vu que $\mathcal{G}_k/k$ est un groupe algébrique connexe de dimension 1 sans torsion, on a donc nécessairement

$$\mathcal{G}_k \cong \mathbb{G}_{a,k}.$$

Pour finir, on va montrer que les conditions $\mathcal{G}_K \cong \mathbb{A}_K^1$ et $\mathcal{G}_k \cong \mathbb{A}_k^1$ impliquent que

$$\mathcal{G} \cong \mathbb{A}_{\mathcal{O}_K}^1.$$

On s'inspire ici de [WW80, Lemma 2.1]. On sait que $\mathcal{G}/\mathcal{O}_K$ est affine. On peut donc écrire $\mathcal{G} = \operatorname{Spec} A$ avec A une $\mathcal{O}_K$-algèbre telle que

$$A \otimes_{\mathcal{O}_K} K = K[t]$$

avec t un élément primitif (i.e. $\Delta(t) = t \otimes 1 + 1 \otimes t$ où Δ est la comultiplication sur $K[t]$). Quitte à multiplier t par un mutliple de π_K, on peut supposer que $t \in A \backslash \pi_K A$. Soient 0_K et 0_k les éléments neutres de $\mathcal{G}_K/K$ et $\mathcal{G}_k/k$ respectivement. On peut supposer que $t(0_K) = 0$ et donc $t(0_k) = 0$. Enfin, on obtient un morphisme

$$\mathcal{G} = \operatorname{Spec} A \to \operatorname{Spec} \mathcal{O}_K[t].$$

Ce morphisme n'est pas constant à la fibre spéciale puisque $t \notin \pi_K A$. Ainsi, c'est un morphisme birationnel et quasi-fini. Comme $\operatorname{Spec} \mathcal{O}_K[t]$ est normal, c'est une immersion ouverte d'après le théorème principal de Zariski (voir [Liu02, Corollary 4.4.6]). Pour obtenir l'isomorphisme annoncé, il reste à démontrer la surjectivité de ce morphisme à la fibre spéciale. Cela résulte du lemme suivant. Enfin, la comultiplication Δ se restreint à $\mathcal{O}_K[t]$ et on a ainsi un isomorphisme de groupes

$$\mathcal{G} \cong \mathbb{G}_{a,\mathcal{O}_K}.$$

□

Lemme 4.2.2. *Soit k un corps. Soit X/k une courbe affine, régulière et de type fini. Alors, toute immersion ouverte*

$$i : X \to X$$

est un isomorphisme.

Démonstration. On peut plonger X dans une courbe projective et régulière $\hat{X}/k$. Alors, i se prolonge en un isomorphisme

$$i : \hat{X} \to \hat{X}.$$

On obtient alors une application surjective

$$\hat{X} \setminus X \to \hat{X} \setminus X$$

qui est bijective car ces ensembles sont finis. Ainsi, i est un isomorphisme. □

4.2.2 Caractéristique résiduelle positive

Proposition 4.2.3. *On suppose que k est de caractéristique $p > 0$. Alors, $\pi_0(\mathcal{G}_k)$ est un p-groupe et on a*

$$\mathcal{G}^0 \cong \mathbb{G}_{a,\mathcal{O}_K}.$$

De plus, tout p-groupe abélien peut être réalisé comme groupe des composantes de la fibre spéciale d'un modèle affine et lisse de $\mathbb{G}_{a,K}/K$.

Démonstration. Pour un entier n premier à p, la multiplication par n sur le groupe algébrique $\mathcal{G}_k^0/k$ est surjective, $\mathcal{G}[n]/\mathcal{O}_K$ est étale et $\mathcal{G}_K(K)[n]$ est trivial. Ainsi, comme dans la démonstration de la proposition 4.2.1, on obtient que $\pi_0(\mathcal{G}_k)[n]$ est trivial pour tout entier n premier à p, i.e. $\pi_0(\mathcal{G}_k)$ est un p-groupe, et que

$$\mathcal{G}^0 \cong \mathbb{G}_{a,\mathcal{O}_K}.$$

Pour démontrer la seconde assertion de la proposition, on utilise la notion de dilatation (voir Section 1.8) pour construire des exemples de modèles de $\mathbb{G}_{a,K}/K$ ayant un groupe des composantes donné. Le procédé est illustré dans la figure 4.1.

Soient $n_1 \geq n_2 \geq \ldots \geq n_r \geq 1$ des entiers. Soient $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathcal{O}_K$ tels que leurs réductions $\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_r \in k$ forment une famille libre sur le sous-corps premier $\mathbb{F}_p$ de k. On considère l'ensemble $\mathcal{E}$ de points de Néron de $\mathbb{G}_{a,K}/K$ défini par le sous-groupe

$$\mathbb{Z} \cdot \alpha_1 + p^{n_1-n_2}\mathbb{Z} \cdot \alpha_2 + \cdots + p^{n_1-n_r}\mathbb{Z} \cdot \alpha_r + p^{n_1}\mathcal{O}_K \subseteq K = \mathbb{G}_{a,K}(K).$$

Par dilatations successives à partir de $\mathbb{G}_{a,\mathcal{O}_K}/\mathcal{O}_K$ on va construire le modèle de Néron $\mathcal{G}/\mathcal{O}_K$ de $\mathbb{G}_{a,K}/K$ associé à $\mathcal{E}$ et montrer que

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}.$$

Plus précisément, à chaque étape on a un modèle $\mathcal{G}/\mathcal{O}_K$ de $\mathbb{G}_{a,K}/K$ et on effectue la dilatation de l'image de la réduction des points $\mathcal{E}$ dans $\mathcal{G}_k/k$. Le procédé s'arrête lorsque l'image de la réduction des points $\mathcal{E}$ dans $\mathcal{G}_k/k$ est dense.

Soit $|\cdot|_K$ une valeur absolue sur K associée à la valuation v_K (normalisée de sorte que $v_K(\pi_K) = 1$). On effectue la dilatation du sous-schéma en groupes fermé $\mathbb{F}_p \cdot \bar{\alpha}_1$ de $\mathbb{G}_{a,k}/k$ dans $\mathbb{G}_{a,\mathcal{O}_K}/\mathcal{O}_K$ avec un rayon $|p|_K$, c'est-à-dire on dilate $\mathbb{F}_p \cdot \bar{\alpha}_1$ puis on dilate $v_K(p) - 1$ fois l'origine de la fibre spéciale ainsi que ses translatés dans chaque composante connexe. On obtient alors un modèle $\mathcal{G}/\mathcal{O}_K$ de $\mathbb{G}_{a,K}/K$ tel que

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p\mathbb{Z}.$$

On dilate ensuite (avec un rayon $|p|_K$) le sous-schéma en groupes fermé de $\mathcal{G}_k$ formé des points de $\mathbb{F}_p \cdot \bar{\alpha}_1$ dans $\mathcal{G}_k^0/k$ ainsi que de leurs translatés dans chaque composante connexe de $\mathcal{G}_k/k$. On obtient un nouveau modèle de $\mathbb{G}_{a,K}/K$, encore noté $\mathcal{G}/\mathcal{O}_K$, avec

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p^2\mathbb{Z}.$$

En effet, on a $\mathcal{G}(\mathcal{O}_K) = \mathbb{Z} \cdot \alpha_1 + p^2\mathcal{O}_K$ et $\mathcal{G}^0(\mathcal{O}_K) = p^2\mathcal{O}_K$. Ainsi, le point α_1 se réduit dans une composante d'ordre p^2. On répète la même opération pour un total de $n_1 - n_2$ fois. On obtient alors un modèle de $\mathbb{G}_{a,K}/K$, toujours noté $\mathcal{G}/\mathcal{O}_K$, avec

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p^{n_1-n_2}\mathbb{Z}.$$

Ensuite, on dilate le sous-schéma en groupes de $\mathcal{G}_k/k$ formé des points de

$$\mathbb{F}_p \cdot \bar{\alpha}_1 + \mathbb{F}_p \cdot \bar{\alpha}_2$$

dans $\mathcal{G}_k^0/k$ ainsi que de leurs translatés dans chaque composante connexe de $\mathcal{G}_k/k$. On obtient un modèle $\mathcal{G}/\mathcal{O}_K$ avec

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p^{n_1-n_2+1}\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

On répète $n_2 - n_3$ fois au total cette opération pour obtenir un modèle $\mathcal{G}/\mathcal{O}_K$ avec

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p^{n_1-n_3}\mathbb{Z} \times \mathbb{Z}/p^{n_2-n_3}\mathbb{Z}.$$

On continue de la même façon jusqu'à la dernière étape qui consistera à dilater n_r fois le sous-schéma en groupes de $\mathcal{G}_k/k$ formé des points de

$$\mathbb{F}_p \cdot \bar{\alpha}_1 + \mathbb{F}_p \cdot \bar{\alpha}_2 + \cdots + \mathbb{F}_p \cdot \bar{\alpha}_r$$

dans $\mathcal{G}_k^0/k$ ainsi que de leurs translatés dans chaque composante connexe de $\mathcal{G}_k/k$.

On obtient comme cela un modèle $\mathcal{G}/\mathcal{O}_K$ de $\mathbb{G}_{a,K}/K$ tel que

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}.$$

De plus, il est clair que $\mathcal{G}/\mathcal{O}_K$ est le modèle de Néron de $\mathbb{G}_{a,K}/K$ associé à l'ensemble de points de Néron $\mathcal{E}$. □

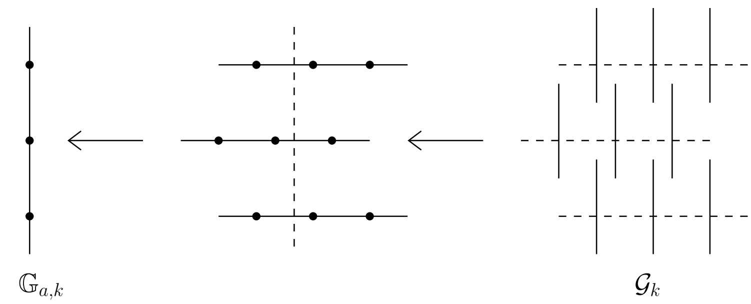

FIGURE 4.1 – Dilatations successives pour obtenir un modèle $\mathcal{G}/\mathcal{O}_K$ de $\mathbb{G}_{a,K}/K$ avec $\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/p^2\mathbb{Z}$ (ici $p = 3$).

4.3 Modèles du groupe multiplicatif

Soit $\mathcal{G}/\mathcal{O}_K$ un modèle affine et lisse de $\mathbb{G}_{m,K}/K$. Le groupe algébrique $\mathcal{G}_k^0/k$ est affine et connexe de dimension 1 et k est algébriquement clos, on a donc $\mathcal{G}_k^0 \cong \mathbb{G}_{m,k}$ ou $\mathcal{G}_k^0 \cong \mathbb{G}_{a,k}$.

4.3.1 Réduction multiplicative

Proposition 4.3.1. *On suppose que $\mathcal{G}_k^0 \cong \mathbb{G}_{m,k}$. Alors, $\mathcal{G}_k/k$ est connexe et on a*

$$\mathcal{G} \cong \mathbb{G}_{m,\mathcal{O}_K}.$$

Démonstration. Soit $\mathcal{T}$ le modèle de Néron localement de type fini de $\mathbb{G}_{m,K}$ (voir [BLR90, Example 10.1.5]). On a

$$\mathcal{T}^0 \cong \mathbb{G}_{m,\mathcal{O}_K}.$$

Comme $\mathcal{G}/\mathcal{O}_K$ est lisse on peut, d'après la propriété de Néron, étendre l'isomorphisme

$$\mathcal{G}_K \cong \mathcal{T}_K$$

en un morphisme birationnel

$$\mathcal{G} \to \mathcal{T}.$$

On note $\mathcal{G}^0$ et $\mathcal{T}^0$ les composantes connexes de 0 de $\mathcal{G}$ et $\mathcal{T}$ respectivement. Soit n un entier premier à p. Comme dans la démonstration de la proposition 4.2.1, on a une injection $\mathcal{G}_k^0(k)[n] \hookrightarrow \mathcal{G}_K(K)[n]$ qui est une bijection par cardinalité. Comme $\mathcal{O}_K$ est hensélien et $\mathcal{T}^0[n]/\mathcal{O}_K$ est fini étale, on a aussi un isomorphisme $\mathcal{T}_k^0(k)[n] \cong \mathcal{T}_K(K)[n]$. On obtient alors un diagramme

$$\begin{array}{ccc} \mathcal{G}_k^0(k)[n] & \cong & \mathcal{G}_K(K)[n] \\ \downarrow & & \downarrow \\ \mathcal{T}_k^0(k)[n] & \cong & \mathcal{T}_K(K)[n] \end{array}$$

où la flèche verticale à droite est un isomorphisme. Ainsi, la flèche verticale à gauche est un isomorphisme et donc le morphisme $\mathcal{G}_k^0 \to \mathcal{T}_k^0$ n'est pas constant. Il est donc quasi-fini. On a alors un morphisme birationnel et quasi-fini

$$\mathcal{G}^0 \to \mathcal{T}^0$$

qui est une immersion ouverte d'après le théorème principal de Zariski. Le morphisme

$$\mathcal{G}_k^0 \to \mathcal{T}_k^0$$

est donc un isomorphisme. D'où un isomorphisme

$$\mathcal{G}^0 \cong \mathcal{T}^0 \cong \mathbb{G}_{m,\mathcal{O}_K}.$$

Comme $\pi_0(\mathcal{G}_k)$ est fini alors que $\pi_0(\mathcal{T}_k) \cong \mathbb{Z}$ est libre, les composantes connexes de $\mathcal{G}_k$ qui ne contiennent pas 0 sont envoyées isomorphiquement sur $\mathcal{T}_k^0$. Le morphisme

$$\mathcal{G} \to \mathcal{T}$$

est donc birationnel et quasi-fini et une nouvelle fois, d'après le théorème principal de Zariski, c'est une immersion ouverte. Ceci implique que $\mathcal{G}_k/k$ est connexe. D'où le résultat escompté. $\square$

4.3.2 Réduction additive

Proposition 4.3.2. *On suppose que* $\mathcal{G}_k^0 \cong \mathbb{G}_{a,k}$.

(1) Si la caractéristique de k *est* 0*, alors* $\pi_0(\mathcal{G}_k)$ *est un groupe cyclique. De plus, tout groupe cyclique peut-être réalisé comme groupe des composantes de la fibre spéciale d'un modèle affine et lisse de* $\mathbb{G}_{m,K}/K$.

(2) Si la caractéristique de k *est* $p > 0$*, alors* $\pi_0(\mathcal{G}_k)$ *est le produit d'un groupe cyclique d'ordre premier à* p *par un* p*-groupe. De plus, tout produit d'un groupe cyclique d'ordre premier à* p *par un* p*-groupe peut-être réalisé comme groupe des composantes de la fibre spéciale d'un modèle affine et lisse de* $\mathbb{G}_{m,K}/K$.

Démonstration. Soit n un entier premier à p. Comme dans la démonstration de la proposition 4.2.1, on a une injection $\mathcal{G}_k(k)[n] \hookrightarrow \mathcal{G}_K(K)[n]$. Comme $\mathcal{G}_K(K)[n]$ est cyclique, $\mathcal{G}_k(k)[n]$ l'est aussi. Ainsi, la partie de $\pi_0(\mathcal{G}_k)$ d'ordre premier à p est cyclique.

Pour construire un modèle ayant un groupe des composantes donné on effectue des dilatations à partir de $\mathbb{G}_{m,\mathcal{O}_K}$. Plus précisément, soit n un entier premier à p et $n_1 \geq n_2 \geq \ldots \geq n_r \geq 1$ des entiers. Pour obtenir

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}),$$

on dilate tout d'abord le sous-schéma en groupes fermé $\mu_{n,k}/k$ de $\mathbb{G}_{m,k}/k$ avec un rayon $|p^{n_1}|_K$. On obtient alors un modèle $\mathcal{G}/\mathcal{O}_K$ de $\mathbb{G}_{m,K}/K$ tel que $\mathcal{G}_k^0 \cong \mathbb{G}_{a,k}$ et

$$\pi_0(\mathcal{G}_k) \cong \mathbb{Z}/n\mathbb{Z}.$$

Ensuite, on effectue les mêmes dilatations que dans la démonstration de la proposition 4.2.3 dans chaque composante connexe de $\mathcal{G}_k/k$ pour construire la partie p-primaire. Avec les mêmes notations, on obtient le modèle de Néron de $\mathbb{G}_{m,K}/K$ associé à l'ensemble $\mathcal{E}$ de points de Néron défini par le sous-groupe

$$\mu_{n,K}(K)(1+p^{n_1}(\mathbb{Z}\cdot\alpha_1+p^{n_1-n_2}\mathbb{Z}\cdot\alpha_2+\cdots+p^{n_1-n_r}\mathbb{Z}\cdot\alpha_r+p^{n_1}\mathcal{O}_K)) \subseteq K^\times = \mathbb{G}_{m,K}(K).$$

□

4.4 Points rationnels du groupe des composantes

On se place maintenant dans le cas d'un corps résiduel non plus algébriquement clos mais fini. Soit $K/\mathbb{Q}_p$ une extension finie de degré d. Soit G/K un groupe algébrique de type fini. Soit $\mathcal{G}/\mathcal{O}_K$ un modèle lisse, de type fini et séparé de G/K. Soit $\pi_0(\mathcal{G}_k)$ le groupe des composantes de la fibre spéciale $\mathcal{G}_k/k$. On s'intéresse ici au sous-groupe des points rationnels de $\pi_0(\mathcal{G}_k)$, c'est-à-dire, aux composantes géométriquement connexes de $\mathcal{G}_k/k$. On se restreint au cas où G/K est le groupe additif $\mathbb{G}_{a,K}/K$ ou le groupe multiplicatif $\mathbb{G}_{m,K}/K$.

4.4.1 Centres et dilatations

On aura besoin du lemme préliminaire suivant sur les dilatations.

Lemme 4.4.1. *Soit $\mathcal{O}_K$ un anneau de valuation discrète de corps résiduel k. Soit $X/\mathcal{O}_K$ un schéma de type fini. Soit Z un sous-schéma fermé de la fibre spéciale X_k/k et soit Y un sous-schéma ouvert et fermé de Z. On note X^Y et X^Z les dilatations de Y et Z dans X respectivement. Alors, on a une immersion ouverte*

$$X^Y \to X^Z.$$

Démonstration. Soit $Y' = Z \setminus Y$. C'est un sous-schéma fermé de X_k. On note $\pi : X^Z \to X$ la dilatation de Z dans X. On va montrer que $X^Z \setminus \pi^{-1}(Y')$ est la dilatation de Y dans X en vérifiant la propriété universelle. Soit S/R un schéma plat et $f : S \to X$ un morphisme tel que $f_k : S_k \to X_k$ se factorise par Y. En particulier, $f_k : S_k \to X_k$ se factorise par Z et il existe donc un unique morphisme $g : S \to X^Z$ tel que $f = \pi \circ g$. Il est évident que l'image de g est en fait contenue dans $X^Z \setminus \pi^{-1}(Y')$, d'où la proposition. □

4.4.2 Modèles du groupe additif

Définition 4.4.2. On appelle *rang* d'un groupe H le cardinal minimal d'une partie génératrice de H.

On note que le rang d'un p-groupe abélien H est égal à la dimension du $\mathbb{F}_p$-espace vectoriel H/pH.

Proposition 4.4.3. *Soit $\mathcal{G}/\mathcal{O}_K$ un modèle affine et lisse de $\mathbb{G}_{a,K}/K$. Alors, le p-groupe $\pi_0(\mathcal{G}_k)(k)$ est de rang $\leq d = [K : \mathbb{Q}_p]$.*

Démonstration. On peut remplacer le schéma en groupes $\mathcal{G}/\mathcal{O}_K$ par le sous-schéma ouvert complémentaire des composantes non géométriquement connexes de la fibre spéciale $\mathcal{G}_k/k$. Celui-ci est stable par la loi de groupes et c'est donc un schéma en groupes dont toutes les composantes de la fibre spéciale sont géométriquement connexes. Le groupe des composantes de ce nouveau schéma est le groupe constant $\pi_0(\mathcal{G}_k)(k)$. Comme dans la démonstration de la proposition 4.2.1, on a un morphisme de groupes birationnel $\mathcal{G} \to \mathbb{G}_{a,\mathcal{O}_K}$. D'après la proposition 1.8.2, ce morphisme se décompose en une composition de n dilatations

$$\mathcal{G} \to \mathcal{G}_{n-1} \to \cdots \to \mathcal{G}_1 \to \mathbb{G}_{a,\mathcal{O}_K}$$

dont les centres sont des sous-schémas en groupes fermés lisses. On obtient cette décomposition de la manière suivante. Soit H_0 l'image de $\mathcal{G}_k$ dans $\mathbb{G}_{a,\mathcal{O}_K}$. Si $H_0 = \mathbb{G}_{a,k}$ alors $\mathcal{G} = \mathbb{G}_{a,\mathcal{O}_K}$. Sinon, on considère $\mathcal{G}_1$ la dilatation de H_0 dans $\mathbb{G}_{a,\mathcal{O}_K}$.

Le morphisme $\mathcal{G} \to \mathbb{G}_{a,\mathcal{O}_K}$ se factorise par $\mathcal{G}_1 \to \mathbb{G}_{a,\mathcal{O}_K}$. Si $\mathcal{G} \to \mathcal{G}_1$ n'est pas un isomorphisme alors on continue en dilatant l'image H_1 de $\mathcal{G}_k$ dans $\mathcal{G}_1$ jusqu'à ce que le procédé termine. Si $\dim(H_{i-1}) = 1$ alors $\mathcal{G}_i \to \mathcal{G}_{i-1}$ est une immersion ouverte et $H_i = \mathcal{G}_{i,k}$. On a alors $\mathcal{G} = \mathcal{G}_i$. Ainsi les centres des dilatations précédentes sont de dimension nulle donc constitués d'un nombre fini de points fermés. Comme les composantes de $\mathcal{G}_k$ sont géométriquement connexes, elles contiennent toutes un point rationnel (on a $H^1(\operatorname{Spec} k, \mathcal{G}_k^0) = 0$ d'après le théorème de Lang et donc une surjection $\mathcal{G}_k(k) \twoheadrightarrow \pi_0(\mathcal{G}_k)(k)$). Ainsi, les centres des dilatations sont constitués uniquement de points rationnels.

D'après le lemme précédent, $\mathcal{G}_1$ est un ouvert du modèle $\mathcal{F}_1/\mathcal{O}_K$ obtenu en dilatant tous les points rationnels de $\mathbb{G}_{a,k}$ dans $\mathbb{G}_{a,\mathcal{O}_K}$. De même $\mathcal{G}_2$ est un ouvert du modèle $\mathcal{F}_2/\mathcal{O}_K$ obtenu en dilatant tous les points rationnels de $\mathcal{F}_{1,k}$ dans $\mathcal{F}_1$. Ainsi de suite, on obtient que $\mathcal{G}$ est un ouvert du modèle $\mathcal{F}_n$ obtenu en dilatant n fois tous les points rationnels de la fibre spéciale. On a donc une injection

$$\pi_0(\mathcal{G})(k) \hookrightarrow \pi_0(\mathcal{F}_n)(k).$$

Il suffit donc de déterminer le rang de $\pi_0(\mathcal{F}_n)(k)$.

Le modèle $\mathcal{F}/\mathcal{O}_K$ est le modèle de Néron de $\mathbb{G}_{a,K}/K$ associé à l'ensemble de points de Néron

$$\mathcal{E} = \mathcal{O}_K + \pi_K^n \mathcal{O}_{K^{\mathrm{nr}}},$$

où π_K est une uniformisante de K, K^{nr} l'extension maximale non ramifiée de K et $\mathcal{O}_{K^{\mathrm{nr}}}$ son anneau d'entiers. On a un morphisme surjectif

$$\mathcal{O}_K = \mathcal{F}_n(\mathcal{O}_K) \twoheadrightarrow \pi_0(\mathcal{F}_n)(k)$$

et donc un morphisme surjectif

$$\mathcal{O}_K/p\mathcal{O}_K \twoheadrightarrow \pi_0(\mathcal{F}_n)(k)/p(\pi_0(\mathcal{F}_n)(k)).$$

Comme la dimension de $\mathcal{O}_K/p\mathcal{O}_K$ sur $\mathbb{F}_p$ est d on a le résultat annoncé. □

4.4.3 Modèles du groupe multiplicatif

Proposition 4.4.4. *Soit $\mathcal{G}/\mathcal{O}_K$ un modèle affine et lisse de $\mathbb{G}_{m,K}/K$. On suppose que $\mathcal{G}_k^0 \cong \mathbb{G}_{a,k}$. Alors, la partie d'ordre premier à p de $\pi_0(\mathcal{G}_k)(k)$, notée $\pi_0(\mathcal{G}_k)(k)'$, est un groupe cyclique d'ordre divisant $|k^\times|$ et la partie p-primaire de $\pi_0(\mathcal{G}_k)(k)$, notée $\pi_0(\mathcal{G}_k)(k)_p$, est de rang $\leq \dim_{\mathbb{F}_p} \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p$. De plus, si l'on note e et f respectivement l'indice de ramification et le degré d'inertie de $K/\mathbb{Q}_p$, on a la majoration*

$$\dim_{\mathbb{F}_p} \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p \leq \frac{pd}{p-1}.$$

Démonstration. De même que dans la démonstration précédente, on a une injection

$$\pi_0(\mathcal{G})(k) \hookrightarrow \pi_0(\mathcal{F}_n)(k)$$

où $\mathcal{F}_n$ est le modèle de $\mathbb{G}_{m,K}/K$ obtenu en dilatant n fois tous les points rationnels de la fibre spéciale à partir de $\mathbb{G}_{m,\mathcal{O}_K}$.

Le modèle $\mathcal{F}_n/\mathcal{O}_K$ est le modèle de Néron de $\mathbb{G}_{m,K}/K$ associé à l'ensemble de points de Néron

$$\mathcal{E} = \mathcal{O}_K^\times(1 + \pi_K^n \mathcal{O}_{K^{\mathrm{nr}}}).$$

On a un morphisme surjectif

$$\mathcal{O}_K^\times = \mathcal{F}_n(\mathcal{O}_K) \twoheadrightarrow \pi_0(\mathcal{F}_n)(k).$$

Comme l'image de $1 + \pi_K\mathcal{O}_K$ dans $\pi_0(\mathcal{F}_n)(k)$ est d'ordre une puissance de p on obtient un morphisme surjectif

$$\mathcal{O}_K^\times/(1 + \pi_K\mathcal{O}_K) \cong k^\times \twoheadrightarrow \pi_0(\mathcal{F}_n)(k)/\pi_0(\mathcal{F}_n)(k)_p \cong \pi_0(\mathcal{F}_n)(k)',$$

d'où le résultat sur la partie d'ordre premier à p. On obtient aussi un morphisme surjectif

$$\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p \twoheadrightarrow \pi_0(\mathcal{F}_n)(k)/p(\pi_0(\mathcal{F}_n)(k)) \cong \pi_0(\mathcal{F}_n)(k)_p/p(\pi_0(\mathcal{F}_n)(k))_p,$$

d'où le résultat sur la partie p-primaire.

Il reste à majorer le rang de $\pi_0(\mathcal{G}_k)(k)_p$. On remarque tout d'abord que

$$\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p \cong (1 + \pi_K\mathcal{O}_K)/(1 + \pi_K\mathcal{O}_K)^p.$$

On considère la série formelle

$$g(X) = (1 + X)^{\frac{1}{p}} = \exp(\frac{1}{p}\log(1 + X)).$$

Pour x tel que

$$v_K(x) > \frac{pe}{p-1}$$

la série $g(x)$ converge dans $1 + \pi_K\mathcal{O}_K$ puisqu'on a alors

$$v_K(\frac{1}{p}\log(1 + x)) \geq v_K(x) - v_K(p) > \frac{e}{p-1}.$$

On note $N = \lfloor \frac{pe}{p-1} \rfloor$. On a donc $1 + \pi_K^{N+1}\mathcal{O}_K \subseteq (1 + \pi_K\mathcal{O}_K)^p$ d'où une surjection

$$(1 + \pi_K\mathcal{O}_K)/(1 + \pi_K^{N+1}\mathcal{O}_K) \twoheadrightarrow (1 + \pi_K\mathcal{O}_K)/(1 + \pi_K\mathcal{O}_K)^p.$$

Maintenant, le rang de $(1 + \pi_K\mathcal{O}_K)/(1 + \pi_K^{N+1}\mathcal{O}_K)$ est $\leq fN \leq \frac{pd}{p-1}$, d'où la majoration annoncée. $\square$

Chapitre 5

Conducteur efficace

Soient K un corps muni d'une valuation discrète v_K, $\mathcal{O}_K$ l'anneau des entiers de K et k son corps résiduel supposé parfait. Soient X/K une courbe propre, lisse et géométriquement connexe, $\mathcal{X}/\mathcal{O}_K$ un modèle propre, régulier et plat de X/K. Soient $\Omega^1_{\mathcal{X}/\mathcal{O}_K}$ le faisceau des différentielles relatives et $\omega_{\mathcal{X}/\mathcal{O}_K}$ le faisceau canonique relatif de $\mathcal{X}/\mathcal{O}_K$. On dispose d'un morphisme canonique

$$H^0(\mathcal{X}, \Omega^1_{\mathcal{X}/\mathcal{O}_K}) \to H^0(\mathcal{X}, \omega_{\mathcal{X}/\mathcal{O}_K})$$

qui est un isomorphisme sur la fibre générique (voir Proposition 1.9.2). Son conoyau est donc de longueur finie sur $\mathcal{O}_K$ et on peut définir la notion de conducteur efficace suivant [LS00].

Définition 5.1. On appelle *conducteur efficace* de X/K l'entier

$$F(X/K) = \ell_{\mathcal{O}_K} \operatorname{Coker}(H^0(\mathcal{X}, \Omega^1_{\mathcal{X}/\mathcal{O}_K}) \to H^0(\mathcal{X}, \omega_{\mathcal{X}/\mathcal{O}_K})).$$

D'après [LS00, Lemma 4], cette définition ne dépend pas du modèle $\mathcal{X}/\mathcal{O}_K$ mais uniquement de X/K.

Le résultat principal de [LS00] est le suivant.

Théorème 5.2. *[LS00, Theorem 0]*

On suppose que la fibre spéciale $\mathcal{X}_k/k$ n'est pas une fibre multiple. Alors, on a

$$F(X/K) \leq f(X/K)$$

où $f(X/K)$ est le conducteur d'Artin de X/K (voir définition 1.5.9).

À la fin de [LS00], Liu et Saito considèrent l'exemple d'une courbe elliptique E/K qui a réduction de type **II**. Lorsque la caractéristique résiduelle de K est

2, ils obtiennent un encadrement du conducteur efficace $F(E/K)$ en fonction du conducteur d'Artin $f(E/K)$. Plus précisément, ils montrent que dans ce cas on a

$$\lfloor (f(E/K)+2)/4 \rfloor \leq F(E/K) \leq \lfloor f(E/K)/2 \rfloor, \tag{5.1}$$

où $\lfloor \cdot \rfloor$ désigne la partie entière. On montrera ici que cet encadrement est optimal parmi les courbes elliptiques à réduction de type **II** en caractéristique résiduelle 2 et que le conducteur efficace $F(E/K)$ ne peut pas s'exprimer uniquement en fonction du conducteur d'Artin $f(E/K)$.

Proposition 5.3. *On suppose que k est de caractéristique 2. Soit E/K une courbe elliptique donnée par une équation de Weierstrass minimale de la forme*

$$y^2 + a_1xy = x^3 + a_6$$

avec $a_1, a_6 \in \mathcal{O}_K$ tels que $v_K(a_1) \geq 1$ et $v_K(a_6) = 1$. On note $F = F(E/K)$ le conducteur efficace et $f = f(E/K)$ le conducteur d'Artin de E/K. On note aussi $v = v_K(a_1)$ et $e = v_K(2)$ l'indice de ramification absolu de K ($e = +\infty$ si K est de caractéristique 2). On a alors le tableau de valeurs suivant :

	F	f
$e < v$	$e+1$	$4e+2$
$2e/3 < v \leq e$	$2e-v+1$	$4e+2$
$v \leq 2e/3$	$2v+1$	$6v+1$

En particulier, l'encadrement (5.1) est optimal.

Démonstration. D'après l'algorithme de Tate, E/K a réduction de type **II**. On reprend le raisonnement de l'exemple à la fin de [LS00]. Soit $\mathcal{X}/\mathcal{O}_K$ le modèle propre et régulier minimal de E/K. La fibre spéciale $\mathcal{X}_k/k$ a un unique point singulier $P = (0,0)$ qui est rationnel. On note pour simplifer $\Omega = \Omega^1_{\mathcal{X}/\mathcal{O}_K}$ et $\omega = \omega_{\mathcal{X}/\mathcal{O}_K}$. Comme ω est un faisceau inversible le noyau du morphisme canonique

$$\Omega \to \omega$$

est le sous-module $\Omega_{\text{tors}} \subseteq \Omega$ des éléments de $\mathcal{O}_X$-torsion. D'après [LS00, Lemma 1], on a $\Omega_{\text{tors}} = 0$ et on sait que ω/Ω est à support dans P. D'après [LS00, Lemma 3], en prenant la cohomologie de la suite exacte

$$0 \to \Omega \to \omega \to \omega/\Omega \to 0$$

on obtient la suite exacte

$$0 \to H^0(\mathcal{X}, \Omega) \to H^0(\mathcal{X}, \omega) \to \omega_P/\Omega_P \to H^1(\mathcal{X}, \Omega)_{\text{tors}} \to 0.$$

D'après [LS00, Corollary 2] et [Liu94, Proposition 1], on obtient

$$f = \ell_{\mathcal{O}_K}(\omega_P/\Omega_P).$$

En divisant l'isomorphisme $\omega \cong \mathcal{O}_X$ par un générateur, l'injection

$$H^0(\mathcal{X}, \omega)/H^0(\mathcal{X}, \Omega) \to \omega_P/\Omega_P$$

s'écrit

$$\mathcal{O}_K/\pi_K^F\mathcal{O}_K \to \mathcal{O}_K[x,y]_{(\pi_K,x,y)}/(y^2 + a_1xy - x^3 - a_6, 2y + a_1x, 3x^2 - a_1y),$$

où π_K est une uniformisante de K. On note A l'anneau de droite ci-dessus. Soit $\mathfrak{m}$ son idéal maximal et soit N le plus petit entier tel que $\mathfrak{m}^N = 0$. On a

$$f = \ell_{O_K}(A) = 1 + \sum_{i=1}^{N-1} \dim_k(\mathfrak{m}^i/\mathfrak{m}^{i+1}). \tag{5.2}$$

Quant à F, c'est le plus petit entier tel que $\pi_K^F = 0$ dans A.

Calculons les entiers f et F. Le discriminant minimal de E/K est

$$\Delta = -a_1^6a_6 - 2^43^2a_6^2.$$

D'après la formule de Ogg-Saito (voir Théorème 1.5.8), on a

$$f = v_K(\Delta).$$

En comparant $v_K(a_1^6a_6) = 6v + 1$ et $v_K(2^43^2a_6^2) = 4e + 2$, on obtient la colonne de droite du tableau comme annoncée.

Avec les relations $2y = -a_1x$ et $3x^2 = a_1y$ on obtient $2y^2 = -3x^3$. Avec la relation $y^2 - x^3 = a_6(1 - (a_1/a_6)xy)$ on a alors $\pi_KA = y^2A$.

Traitons le cas où $e < v$. La relation $2y = -a_1x$ dans A implique que

$$y^{2e+1}A = 2yA \subseteq a_1A = \pi_K^vA \subseteq y^{2e+2}A$$

et donc $y^{2e+1} = 0$. Alors, $\pi_K^{e+1} = 0$ dans A et donc $F \leq e + 1$. Il y a en fait égalité compte tenu de l'encadrement (5.1) et de l'égalité $\lfloor (f + 2)/4 \rfloor = e + 1$. En particulier, on atteint ici la borne inférieure de l'encadrement (5.1).

Supposons maintenant que $e \geq v$. On a $\mathfrak{m} = xA + yA$ et $x^2 \in \pi_KA = y^2A$ d'où $\mathfrak{m}^i = xy^{i-1}A + y^iA$ pour tout $i \geq 1$. La relation $a_1x = -2y$ implique que $xy^{2v}A \subseteq y^{2e+1}A \subseteq y^{2v+1}A$. Ainsi, $\mathfrak{m}^i = y^iA$ pour tout $i \geq 2v + 1$. On montre dans le lemme suivant qu'il n'y a pas de relation entre y^{2v} et xy^{2v-1} modulo $\mathfrak{m}^{2v+1}$. On obtient donc, d'après la formule (5.2),

$$f = 1 + 2 \cdot 2v + (N - 1 - 2i) = N + 2v. \tag{5.3}$$

Montrons que $F > v$. On suppose par l'absurde que $F \leq v$. Comme $y^{2F} = 0$ dans A on a $\mathfrak{m}^{2F+1} = 0$. D'après la formule (5.3), on a alors $f \leq 2F+1+2v \leq 4v+1$. Si $v \leq 2e/3$ alors $f = 6v+1$ et on a une contradiction. Si $v > 2e/3$ alors $f = 4e+2$ et $4v+1 \leq 4e+1$ et on a encore une fois une contradiction.

Maintenant, d'une part, le fait que $y^{2F} = 0$ dans A implique que $\mathfrak{m}^{2F} = y^{2F}A = 0$ et donc $N \leq 2F$. D'autre part, le fait que $y^{2F-2} \neq 0$ implique que $N > 2F-2$. Ainsi, on a $2F-1 \leq N \leq 2F$, d'où $F = \lfloor (N+1)/2 \rfloor$.

On peut enfin terminer le calcul de F. Pour $v \leq 2e/3$, on a, d'après la formule (5.3), $N = f - 2v = 4v+1$, d'où $F = 2v+1$. Pour $v > 2e/3$, on a $N = 4e+2-2v$, d'où $F = 2e - v + 1$. D'où la deuxième colonne du tableau.

On a déjà vu que l'on atteint la borne inférieure de l'encadrement (5.1) dans le cas où $e < v$. Dans le cas où $v = 1$ et $e \geq 2$ on a

$$F = 2v + 1 = 3 = \lfloor (6v+1)/2 \rfloor = \lfloor f/2 \rfloor.$$

Ainsi la borne supérieure est elle aussi atteinte et donc l'encadrement (5.1) est optimal. □

Remarque 5.4. La deuxième ligne du tableau montre que le conducteur efficace $F(E/K)$ ne dépend pas que du conducteur d'Artin $f(E/K)$.

Lemme 5.5. *On considère l'anneau*

$$\hat{A} = \mathcal{O}_K[[x,y]]/(y^2 + a_1xy - x^3 - a_6, 2y + a_1x, 3x^2 - a_1y) \cong A,$$

avec $a_1, a_6 \in \mathcal{O}_K$ tels que $v_K(a_1) \geq 1$ et $v_K(a_6) = 1$. Soit $\mathfrak{m}$ son idéal maximal. On note $v = v_K(a_1)$ et $e = v_K(2)$ et on suppose que $v \leq e$. Alors, les images de y^{2v} et xy^{2v-1} dans le k-espace vectoriel $\mathfrak{m}^{2v}/\mathfrak{m}^{2v+1}$ forment une base.

Démonstration. On a vu dans la démonstration précédente que $\mathfrak{m}^{2v+1} = y^{2v+1}\hat{A}$. Supposons qu'existent $a, b \in \mathcal{O}_K$ et $R, S, T, U \in \mathcal{O}_K[[x,y]]$ tels que

$$ay^{2v} + bxy^{2v-1} = Uy^{2v+1} + R(y^2 + a_1xy - x^3 - a_6) + S(2y + a_1x) + T(3x^2 - a_1y).$$

Soit $\alpha_i \in \mathcal{O}_K$ le coefficient de y^{2i} dans R. Par identification des coefficients des séries formelles, on obtient les relations

$$\begin{aligned} a &= \alpha_{v-1} - a_6\alpha_v \bmod \pi_K^v, \\ 0 &= \alpha_{i-1} - a_6\alpha_i \bmod \pi_K^v \text{ pour } 1 \leq i < v, \\ 0 &= \alpha_0. \end{aligned}$$

Ainsi, en remontant ces relations, on obtient $\pi_K^{v-1}|\alpha_1$, $\pi_K^{v-2}|\alpha_2$ et ainsi de suite jusqu'à $\pi_K|\alpha_{v-1}$. D'où, $\pi_K|a$.

De même, soit $\beta_i \in \mathcal{O}_K$ le coefficient de xy^{2i-1} dans R. Par identification des coefficients, on obtient les relations

$$\begin{aligned}
&b = \beta_{v-1} - a_6\beta_v \bmod \pi_K^v,\\
&0 = \beta_{i-1} - a_6\beta_i \bmod \pi_K^v \text{ pour } 2 \leq i < v,\\
&0 = \beta_1 \bmod \pi_K^v.
\end{aligned}$$

Ainsi, en remontant ces relations, on obtient $\pi_K^{v-1}|\beta_1$, $\pi_K^{v-2}|\beta_2$ et ainsi de suite jusqu'à $\pi_K|\beta_{v-1}$. D'où, $\pi_K|b$.

Le résultat annoncé en découle. $\square$

Références

[AW71] M. Artin et G. Winters, *Degenerate fibres and stable reduction of curves*, Topology **10** (1971), 373-383.

[BLR90] S. Bosch, W. Lütkebohmert et M. Raynaud, *Néron Models*, Ergeb. Math. Grenz. **21**, Springer, 1990.

[BX96] S. Bosch et X. Xarles, *Component groups of Néron models via rigid uniformization*, Math. Ann. **306** (1996), 469-486.

[BK94] A. Brumer et K. Kramer, *The conductor of an abelian variety*, Comp. Math. **92** (1994), 227-248.

[Cha00] C.-L. Chai, *Néron models for semiabelian varieties : congruence and change of base field*, Asian Journal of Math. **4** (2000), 715-736.

[CY01] C.-L. Chai et J.-K. Yu, *Congruences of Néron models for tori and the Artin conductor*, avec un appendice de E. de Shalit, Ann. of Math. **154** (2001), 347-382.

[CX08] P. L. Clark et X. Xarles, *Local bounds for Torsion Points on Abelian Varieties*, Canad. J. Math. **60(3)** (2008), 532-555.

[CGP10] B. Conrad, O. Gabber et G. Prasad, *Pseudo-reductive Groups*, New Math. Monographs **17**, Cambridge University Press, 2010.

[DW74] I. Dolgacev et B. Weisfeiler, *Unipotent group schemes over integral rings*, Izv. Akad. Nauk SSSR Ser. Mat. **38(4)** (1974), 757–799.

[Edi92] B. Edixhoven, *Néron models and tame ramification*, Compos. Math. **81** (1992), 291-306.

[ELL96] B. Edixhoven, Q. Liu et D. Lorenzini *The p-part of the group of components of a Néron model*, J. Alg. Geom. **5(4)** (1996), 801-813.

[EHN15] D. Eriksson, L. H. Halle et J. Nicaise, *A logarithmic interpretation of Edixhoven's jumps for Jacobians*, Adv. Math. **279** (2015), 532-574.

[Fal08] G. Faltings, *Néron Models and Formal Groups*, Milan J. Math. **76** (2008), 93-123.

[HN10] L. H. Halle et J. Nicaise, *The Néron component series of an abelian variety*, Math. Ann. **348(3)** (2010), 749-778.

[HN11] L. H. Halle et J. Nicaise, *Motivic zeta functions of abelian varieties, and the monodromy conjecture*, Adv. Math. **227** (2011), 610-653.

[HN16] L. H. Halle and J. Nicaise, *Néron models and base change*, Lecture Notes in Mathematics **2156**, Springer, 2016.

[Haz78] M. Hazewinkel, *Formal Groups and Applications*, Pure and Applied Math. **78**, Academic Press, 1978.

[Her16] A. Hertgen, *Splitting properties of the reduction of semi-abelian varieties*, à paraître dans International Journal of Number Theory.

[Kat73] N. Katz, *p-Adic Properties of Modular Schemes and Modular Forms*, Lect. Notes Math. **350**, Springer, 1973.

[Liu02] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Grad. Texts Math. **6**, Oxford University Press, 2002.

[Liu94] Q. Liu, *Conducteur et discriminant minimal de courbes de genre 2*, Compositio Math. **94** (1994), 51-79.

[LL01] Q. Liu et D. Lorenzini, *Special fibers of Néron models and wild ramification*, J. reine. angew. Math. **532** (2001), 179-222.

[LLR04] Q. Liu, D. Lorenzini et M. Raynaud, *Néron models, Lie algebras, and reduction of curves of genus one*, Inv. Math. **157** (2004), 455-518.

[LS00] Q. Liu et T. Saito, *Inequality for conductor and differentials of a curve over a local field*, J. Alg. Geom. **9** (2000), 409-424.

[LRS93] P. Lockhart, M. Rosen et J. H. Silverman, *An upper bound for the conductor of an abelian variety*, J. Alg. Geom. **2** (1993), 569-601.

[Lor10] D. Lorenzini, *Models of curves and wild ramification*, Pure Appl. Math. Q. **6** (2010), no. 1, Special Issue : In honor of John Tate, Part 2, 41-82.

[Loz13] À. Lozano-Robledo, *Formal Groups of Elliptic Curves with Potential Good Supersingular Reduction*, Pacific J. Math. **261(1)** (2013), 145-164.

[Lut16] W. Lütkebohmert, *Rigid Geometry of Curves and Their Jacobians*, Ergeb. Math. Grenz. **61**, Springer, 2016.

[Mat55] A. Mattuck, *Abelian Varieties over p-Adic Ground Fields*, Ann. of Math. **62** (1955), 92-119.

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177-190.

[NX91] E. Nart et X. Xarles, *Additive reduction of algebraic tori*, Arch. Math. **57** (1991), 460-466.

[Né64] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. Math. IHES **21** (1964), 1-128.

[Ogg67] A. P. Ogg, *Elliptic curves and wild ramification*, Am. J. Math. **89** (1967), 1-21.

[Sai88] T. Saito, *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J. **57** (1988), 151-173.

[SGA3] J.-E. Bertin, *Généralités sur les schémas en groupes*, Séminaire de Géométrie Algébrique du Bois Marie 1962-64 : Schémas en groupes, Tome 1, Exposé VIB, Documents Mathématiques **7**, Société Mathématique de France, 2011.

[SGA7] A. Grothendieck, *Modèles de Néron et monodromie*, Séminaire de Géométrie Algébrique du Bois Marie 1967-69 : Groupes de monodromie en géométrie algébrique, Tome 1, Exposé IX, Lecture Notes in Mathematics **288**, Springer, 1972.

[Ser68] J.-P. Serre, *Corps Locaux*, Hermann, 1968.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. **15** (1972), 259-331.

[Ser85] J.-P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques*, Oeuvres, Volume **II**, 581-592, Springer, 1985.

[ST68] J.-P. Serre et J. Tate, *Good Reduction of Abelian Varieties*, Ann. of Math. **88** (1968), 492-517.

[Sil86] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. **106**, Springer, 1986.

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. **151**, Springer, 1994.

[Tat97] J. Tate, *A review of non-Archimedean elliptic functions*, in Elliptic Curves, Modular Forms, and Fermat's Last Theorem, edited by John H. Coates and Shing-Tung Yau, 162-184, Int. Press, 1997.

[WW80] W. Waterhouse et B. Weisfeiler, *One Dimensional Affine Group Schemes*, Journal of Algebra **66** (1980), 550-568.

Modèles de Néron et groupes formels

Résumé : Dans cette thèse, on aborde plusieurs questions autour des modèles de Néron de variétés abéliennes sur un corps de valuation discrète. On dit qu'une variété abélienne a réduction scindée si la suite exacte définissant le groupe des composantes de la fibre spéciale est scindée. On donne un exemple de variété abélienne modérément ramifiée qui n'a pas réduction scindée. Pour les variétés jacobiennes, on montre que l'on obtient réduction scindée après toute extension modérément ramifiée de degré plus grand qu'une constante ne dépendant que de la dimension. On considère aussi le lien avec le conducteur de Swan. Ensuite, on s'intéresse aux groupes formels des variétés abéliennes. Pour les courbes elliptiques, on détermine le rayon du plus grand voisinage de 0 qui est isomorphe à un polydisque muni de sa structure de groupe usuelle. On s'intéresse aussi aux groupes des composantes de modèles lisses, de type fini et séparés du groupe additif ou multiplicatif ainsi qu'à leurs sous-groupes des points rationnels. Enfin, on montre que le conducteur efficace d'une courbe algébrique ne peut pas s'exprimer uniquement en fonction de son conducteur d'Artin.
Mots-clefs : variété abélienne ; courbe elliptique ; modèle de Néron ; groupe des composantes ; ramification ; conducteurs ; groupe formel ; dilatation.

Néron models and formal groups

Abstract : In this thesis, we tackle several questions about Néron models of abelian varieties on a discrete valuation field. We say that an abelian variety has split reduction if the exact sequence defining the group of components of the special fiber is split. We give an example of a tamely ramified abelian variety which does not have split reduction. For Jacobian varieties, we show that one gets split reduction after any tamely ramified extension of degree greater than a constant depending on the dimension only. We also consider the link with the Swan conductor. Then, we deal with formal groups of abelian varieties. For elliptic curves, we compute the radius of the largest neighbourhood of 0 which is isomorphic to a polydisk equipped with its usual group law. We also deal with groups of components of smooth and separated models of finite type of the additive or multiplicative group as well as their subgroups of rational points. Finally, we show that the efficient conductor of an algebraic curve cannot be expressed in terms of its Artin conductor only.
Keywords : abelian variety; elliptic curve; Néron model; group of components; ramification; conductors; formal group; dilatation.
Institut de Mathématiques de Bordeaux UMR 5251
Université de Bordeaux
351, cours de la Libération - F 33 405 TALENCE